Acceptable Use Policy

Each year it is our practice to send out a reminder to all Banner HR users to be especially careful with the access, review and disposition of sensitive employee information which includes, but is not limited to data about birthdates, annual or hourly salary, benefits, and social security numbers. Please note that USNH has adopted a classification model which provides definitions for data which is either restricted (legally protected), sensitive (data USNH protects or agrees to protect through contract), or public (approved for viewing by the public). The model and full definitions of each category can be found at the link below:

http://it.unh.edu/media/IT%20Security/Data_Classificaton_Policy_11202008.pdf

Each campus has an Acceptable Use Policy. In some cases, it is the campus practice to require the user to sign a form to acknowledge they have read and understood the parameters of appropriate computer use on their campus. For your information, the links below will bring you to the Acceptable Use Policy for Granite State College, Keene, Plymouth and UNH:

http://www.keene.edu/policy/cnup.cfm
http://www.plymouth.edu/infotech/policy/PSU/accept.html
http://usnholpm.unh.edu/UNH/VI.Prop/F.htm#5
http://www.granite.edu/library/pdf/current-students/policies-and-procedures/ComputerNetworkPolicy.pdf

These four policies, in conjunction with the clear rules established in the USNH Policies and Procedures Manual regarding the disclosure and use that will be made of recorded personnel data, provide the framework for an employee's responsibilities and stewardship regarding information technology. Another good reference is the new USNH System Access Policy which is intended to serve as guidelines for the protection of sensitive information (e.g., this policy explicitly prohibits emailing an employee's Social Security Number). The link below will provide you with a copy of this policy and an explanation of the minimum compliance standards that should be used by all employees:

http://www.usnh.edu/olpm/USY/VI.Prop/F.htm

In general, privacy of personnel information is a matter of growing concern, and in today's culture, it is not uncommon to receive questions regarding how this information will be used by employers. All employees have the right to feel confident that their personnel information is maintained in a manner that is accurate, and as restricted to "need to know" use as legally appropriate. Banner HR users not only have specific rights as employees regarding personnel information in their files, but also have a strong obligation to protect the confidentiality of people for whom they process or access personnel documentation. In fact, the State of NH has instituted a data breach reporting requirement if sensitive information is disclosed to unauthorized persons. And, while the policies above speak in general terms about data, I would like to use this opportunity to remind you of the following good practices as it relates to Banner HR and personnel data:

- Try to request and use only that personnel information that is related to your specific business need;
- Consider personnel information to be confidential. The dissemination of personnel information, except for those records covered by the NH Right-to-Know and those covered by HIPAA, should be done on a "need-to-know" basis. (Records covered by the Right to Know law may be released without employee consent or need to know. HIPAA covered records must have an employee release, regardless of the organizational need to know).
- Restrict access to any personnel record to those who have proper authorization and legitimate business reason, unless otherwise required by law or legal process;
- Make sure that actions of decisions are based upon pertinent and accurate data;
- Communicate to employees their responsibilities in handling personnel information in accordance with the principles found in the USNH Policies and Procedures manuals;
- Avoid corrupting the data of employee records.

I am happy to report that USNH no longer uses an employee's Social Security Number (SSN) as the primary identifier in the Banner HR and Finance systems. With rare exception, an employee should always be identified by this new USNH ID, and it is safe to display the full and unique nine-digit number in all correspondence. If an employee cannot remember their new USNH ID, it can easily be found on WISE (www.wise.unh.edu). We have also worked with

our Management Reporting team to ensure that the USNH ID has replaced the SSN on all non-regulatory corporate reports.

As a good business practice, documents that include any sensitive data about employees should not be distributed beyond individuals who have demonstrated a legitimate business need for this information. Try to incorporate the following practices into your daily routine:

- Please be careful that you do not share or distribute reports if there is no business requirement for the data. This pertains to both reports that include the new USNH ID, or to the limited number of reports that still must include the SSN due to regulatory requirements. Reports should not left in a public or private location where they can be viewed by the casual observer.
- Banner HR screenshots are often sent to central offices to assist with troubleshooting, and central staff have been trained to associate employees with their new USNH ID. If there are questions, you are encouraged to try to resolve the matter by phone.
- If, in very extreme circumstances, you need to transmit the SSN, the System Access Policy requires this number be encrypted. This can be accomplished by pasting the screen print into a word document and sending that document with a secure password. The UNH Office of IT Security can assist with training on encrypting documents.

We have received questions regarding the proper disposal of HR documentation that includes sensitive data. This material should not be put in a regular office waste basket -- it should be shredded, destroyed, or placed in specially designated bins for later destruction. This practice is appropriate even if the material contains only information such as title and salary that may otherwise be open to dissemination via NH's Right-to-Know law.