

## 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 birth date, annual or hourly salary, benefits, and social security numbers.

You will note that 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/accept.html>

<http://www.unh.edu/cis/aup.html>

[Granit State College Computer & Network Acceptable Use Policy](#)

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.

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. 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.

As a general practice, documents that include the employee's social security number (SSN) 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:

- Try not to transmit an individual's full SSN via any medium (paper, fax, email, etc.). The appropriate practice is to include only the last four digits of the number. Banner HR users can almost always identify the correct person with only this piece of the SSN. If there is a problem, the practice should be to telephone the initiator for additional information;
- MR corporate and ad hoc reports rely heavily on the use of an employee's SSN and display very sensitive employee information. These reports should not be shared or distributed to individuals who do not have a business need for the data, and it is important that the reports not be left in a public or private location where they can be viewed by the casual observer. As MR develops new reports or modifies existing reports, the practice will be to mask the employee's SSN whenever possible by only displaying the last four digits of the number;
- Banner HR screenshots are often sent to central offices to assist in troubleshooting various problems. Here are some good practices to follow if the form includes an employee's SSN:
  - Consider purchasing software that allows the user to capture and edit the image (e.g., 'Snag It') and use this to blank out any sensitive data from the document before transmittal;
  - If transmitted via email and the department has no way to modify the screen print, mark the envelope 'confidential';
  - If printed out and hand delivered or sent via fax or postal service, blacken out all but the last four digits of the SSN and either put the document in an envelope marked confidential or place face down in a secure location;

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.

Thanks for taking the time to review these general practice tips.