Community College System of New Hampshire
Information Security and Access Program
(ISAP)

Final Rev. 10/1/10

Purpose of the ISAP

Institutional data is one of the CCSNH's most valuable assets. It is used by our System of Colleges to make operational and budget decisions and to meet State and Federal reporting requirements. It serves as the foundation for strategic thinking and planning. With data breaches on the rise and new laws holding institutions accountable for securing and restricting access to Personally Identifiable Information (PII), it is critical that the CCNSH establish an ISAP.

CCSNH ISAP components:

> Section 1- Information: Describes why the policy exists and why it must be adhered to by those who have access to Personally Identifiable Information (PII). Not all information is PII so the ISAP provides examples of data elements that fall under PII and where PII is found within CCSNH data systems.
>
> Section 2 - Policy: Enhances the protection of PII by defining CCSNH policies, procedures and expectations for employees who handle PII.

Section 1- ISAP Information

Why Do We Need to Secure PII?

It is important to secure PII because data breaches, whether small or large, by accident or by design, can result in long term damage to the CCSNH Colleges' reputations as well as carry stiff financial penalties. Most breaches are internal and accidental, so periodic employee education on best practices for securing PII is critical. Below is a sample of data breaches which exposed PII:

- August 2006, a contract company for the Veteran's Affairs administration lost a laptop computer with the PII of over 16,000 persons.
- 2002 – 2006, a total of 478 laptops were reported lost or stolen from the IRS. The laptops held sensitive taxpayer information including Social Security Numbers.
- August 4, 2010, Hingham city government, Hingham, Massachusetts. An email with the Social Security numbers, names, and employee identification numbers of 1300 city

employees was accidentally emailed to about 30 department heads. Some of the emails were automatically forwarded to personal accounts and personal devices.

- June 29, 2010, Fort Worth Allergy and Asthma Associates. Theft of four computers resulted in 25,000 patient records being exposed. The patient records contained addresses, Social Security numbers and dates of birth.
- August 2010, College Center for Library Automation, Florida. Personal data from 126,000 students, faculty and staff from six colleges was accessible through the Internet for five days. The information may have included full names, Social Security numbers, driver's license numbers, and Florida identification card numbers. It was determined that the installation of a software upgrade left the personal data unintentionally accessible.

There are numerous other examples. It should be noted that many data breaches are the result of stolen or misplaced portable devices or media which can store large amounts of data such as laptops, USB storage devices (e.g., hard drives, thumb drives), and CDs/DVDs. Simply limiting the amount of laptops we issue will reduce our overall risk.

In addition to the concern about PII falling into the wrong hands, there is also the cost of protecting the identity of those exposed by the data breach:

- In a 2006 study it was determined that the average cost for companies to provide Identity Theft Protection was **$140 per lost customer record**. Multiply this amount across many thousands of records in a single electronic data breach and the costs become significant. Also, Identity Theft Protection is like insurance – the expense is still incurred whether or not any of the lost PII is ever used for illegal purposes.

Most importantly for our colleges there is an increasing public awareness about the risk of data breaches and identity theft with an expectation that our institutions are taking the necessary precautions to secure their personal information. This awareness has resulted in new legislation which squarely places the accountability for securing PII on those who collect and store information containing PII.

What is PII?

Not all information needs to be protected as PII. In general, any information that could reasonably be used to identify a person is considered "***personally identifying information***." This may include, but is not limited to (***excerpt from the NH Privacy Statement*** on the CCNSH web page):

- Name (full name, maiden name or alias);
- Address (excluding zip code);
- E-mail address;

- Social security number;
- Passwords;
- Bank account information;
- Credit card information;
- License or identification number;
- Telephone number;
- Medical or disability information;
- Any combination of data that could be used to identify a person such as birth date, zip code and gender; and
- Any graphical or visual representation of a person.

Note 1: Some of these data elements on their own are enough to positively identify a person (e.g., Social Security Number) while others like "Name" is not. However, it is also the minimum combination of data elements that we must be aware of when protecting PII. For example, a combination of **"Name"+"Address"+"DOB"** could be enough data elements to positively identify a person without a Social Security Number but those data elements on their own would not.

Also, the **context** of how PII is used can determine if it should be secured. For example, a list of names subscribing to a college newsletter would not be considered sensitive PII which needs to be secured. However, a list of names of those receiving treatment for substance abuse would fall under PII which needs to be secured.

Note 2: CCSNH Employees and PII. Personally identifiable information refers to information which can be used to distinguish or trace an individual's "personal" identity. Employee information such as home address, personal phone numbers and other "personal" information is considered PII which must be protected and secured like any other PII. Business assigned identifiers such as office telephone and FAX numbers, business cell phone numbers, Email addresses, business addresses or identification cards displaying employee names and images are not considered sufficiently sensitive to require PII protection. These business identifiers may be responsibly published and distributed by the CCSNH to be used by our educational community, by the public or provided as required by law.

Where is PII Located?

For the CCSNH the majority of the data elements considered PII are kept in and secured by **Banner;** therefore **Banner** is a major focus of the ISAP policy. However, if Banner is identified as the "headwaters" for CCSNH data, it may feed other systems or reports. It is important that extra measures are taken to identify and secure downstream "pools" of data that are no longer under the security blanket of **Banner**. For example;

- A user may download a report from **Banner** containing PII, save it to a laptop, to a portable device/media or print it on a piece of paper which becomes lost or stolen.
- A College ID card system server is fed data containing PII from **Banner** but access policies for the College server are poorly defined which could expose PII to unauthorized personnel.

Also, departments may collect data containing PII not intended for input into **Banner**. The data may exist on a spreadsheet or in a small database or in a program the department uses. **As long as the CCSNH collects and stores data which may contain PII (in Banner, outside of Banner or on paper) there is responsibility and accountability for securing that data wherever it exists.**

How do we secure PII?

PII found in Banner:

SCT **Banner** is the major higher education software provider in the market. While their software may seem arcane at times, it is important to note they have been very successful at storing, presenting and securing data kept in **Banner.** As long as access to **Banner** is controlled properly by the System Office and the Colleges, **Banner** manages the rest. The required process to obtain a **Banner** account may appear restrictive. The restrictions are present to ensure authorized employees receive the appropriate level of **Banner** data access, based upon work responsibilities. Access is managed and updated in a secure manner as well.

PII Outside the Security of Banner:

The **Banner** system is designed to store and secure PII. **Banner** should be given the first priority when considering where College data is maintained. However, today's reality is users often need access to data through online services which may not be as secure as **Banner**. If it is absolutely critical that data containing PII be stored or shared outside of **Banner,** certain restrictions apply as noted in the ISAP policy.

========== Section 2 ==========

Community College System of New Hampshire

Section**: Human Resources**	Subject: **Information Security and Access**
Policy: **CCSNH Information Security and Access Program Policy**	Date Approved:
Policy #:	Date of Last Amendment:
	Effective Date: 10/1/2010
Approved: Richard A. Gustafson, Chancellor	

I. Banner Access:

Banner access is restricted to CCSNH employees or third party contractors who have work related responsibilities requiring that access. Unauthorized or illegitimate use of the **Banner** system or data may result in disciplinary action.

When logging into the **Banner** system, the **Banner** account holder understands and agrees to abide by the following:

A. Access to **Banner** is granted to a CCSNH employee/third party contractor solely to perform appropriate and authorized job functions. Confidentiality of the information/data accessed must be protected. Data should be accessed and/or modified only with a legitimate purpose in completing work assignments.
B. For enhanced security **Banner** passwords are periodically expired and must be re-created (old passwords cannot be recycled). An individual's password(s) must not be shared with or used by any other person who holds a **Banner** account. **Banner** passwords must not be disclosed to any unauthorized individual to gain access to the **Banner** system.
C. When handling Personally Identifiable Information (PII) in paper or electronic formats:
    i. Use of PII should always be as restricted as feasible.
    ii. If you are not at your desk do not leave reports containing PII displayed on your computer screen or unsecured on your desk so others may see their content.
    iii. All paper reports or files containing PII should be secured when not in use and should be shredded or deleted when they are no longer needed.

iv. PII which resides on portable devices (e.g., laptops, USB drives) should always be encrypted. **Upon inquiry, College IT staff will provide information on the CCSNH supported encryption software.**

D. Due to the inherent security risk with wireless connections, access to **Banner** through a wireless connection requires the use of CCSNH issued Virtual Private Network (VPN) software.

E. The CCSNH supplied VPN (Virtual Private Network) software should always be used for remote access to **Banner**. The VPN software provides a private connection through the public Internet. Upon request, College IT staff will provide a copy of the VPN Request Form. Once the Request is approved the VPN software installation process can be done on any authorized CCSNH computer.

F. The CCSNH issued computer should be the only authorized computer used to access the **Banner** system. College IT staff have the responsibility to maintain CCSNH issued computers with automatic software updates. These updates provide Operating System modifications and upgrades, to protect each computer against viruses and other dangerous software which might compromise the computer and any information on it. To enhance security, each CCSNH computer should be used for work related purposes only. **Personally owned computers are not permitted to access the Banner system or other CCSNH data systems storing Personally Identifiable Information, since these computers are not maintained or secured by CCSNH IT.**

II. General Access to Data containing PII:

A. Unless there is a demonstrated need to be mobile with a laptop, **a desktop computer is strongly recommended.** A laptop computer is a frequent target for theft due to its mobility and should not be the first choice to access **Banner** or to store **PII**. If a laptop is required then a lock down cable should be issued and used to secure the laptop.

B. If PII must be stored on a CCSNH issued computer (laptop or desktop) or other storage devices (e.g., external hard drives, USB drives, etc.) this information must be encrypted and password protected using the CCSNH supplied encryption software. Upon request, College IT staff will assist with installation of this software.

C. Personally identifiable information should not be sent using email or FAX facilities unless there are secure processes in place (secure FAX locations, follow up with receiver to be sure the FAX or email has been received, etc.)

D. Copiers and multi-function printers (MFPs) have the ability to store documents/images on internal hard drives which must be permanently deleted by the leasing company or IT before the device is released or discarded. Proof of the deletion is required for College records.

E. When laptops, desktops and other computer equipment capable of storing data are reassigned or discarded, the data must be permanently deleted on the equipment by the

College IT department. Proof of the deletion is required and must be kept with IT records.

F. If data containing PII is maintained outside of **Banner,** in the form of files on a computer or on a storage device, the data must be secured by enterprise encryption software provided by the CCSNH.
G. If data containing PII is shared with another system, reasonable efforts must be made to ensure the other system, if under CCSNH control, is secure. If the other system or entity is not under CCSNH control, appropriate written releases must be obtained to transmit the data. The releases must convey the authority and responsibility of securing the data to the other entity (either through a contract or Memorandum of Understanding) so that the CCSNH no longer retains responsibility for securing the data.
H. Immediately upon termination of employment or contract, employee or third party contractor access (physical or electronic) to data with PII must be removed.
I. If it is questionable whether a system contains PII, the system must be treated as if it does contain PII (the ISAP applies).
J. Any suspicious behavior or potential data breaches such as lost laptops or storage devices with stored Personally Identifiable Information must be reported <u>immediately</u> to the College **Banner** Coordinator or to the System Office **Banner** IT staff (if the **Banner** Coordinator is not available). Once reported, the ***"Data Breach Notification Process"*** must be followed (see below).

III. Data Breach Notification Process

The CCSNH is legally required to notify the New Hampshire Attorney General's Office of any data breaches per **TITLE XXXI TRADE AND COMMERCE CHAPTER 359-C, RIGHT TO PRIVACY**, ***Notice of Security Breach, Section 359-C:20***.

When the **Banner** Coordinator or System Office **Banner** IT staff (or any other person) is notified of a suspected data breach of a CCSNH system, notification must be made to the College President, the CCSNH Chancellor's office and CCSNH legal counsel. **<u>This group must work to:</u>**

A. Identify and document how the breach occurred.
B. Identify the individuals whose Personally Identifiable Information may have been compromised.
C. Identify the potential harm to these individuals by the breach.
D. Determine the impact of the breach and whether external notification is required.
E. Determine ways to assist the individuals affected by the breach.
F. Determine the best notification process to the impacted individuals (the source, content and method).
G. Notify the New Hampshire Attorney General's Office.

H. Follow up: Identify how this process can be improved and how to avoid future data breaches.

IV. ISAP Review, Updates and Employee Awareness

State and federal laws change over time and may affect the handling and storage of PII. Any implementation of new services that access PII must be reviewed for compliance requirements. Any new requirements must be identified and followed.

To remain current, the ISAP must be reviewed annually (or sooner if situations dictate). The CCSNH CIO, in consultation with the Chancellor and the System Leadership Team, must perform this review and update the ISAP as required.

This program, policies and any critical training will be disseminated to all CCSNH employees using the CCSNH Intranet (SysNet).

V. Those Impacted By This Program:

All CCSNH faculty, staff, student workers and contract workers are directly affected by this policy.

VI. References

A. FERPA of 1974 as amended (Also known as Buckley Amendment)
B. The CCSNH IT Acceptable Use Policy - adopted by the CCSNH July 2009
C. Red Flags Policy on Identity Theft - adopted by the CCSNH May 2009
D. **Banner** Data Standards And Guidelines
E. New Hampshire Government website
F. The Community College System of New Hampshire website
G. Massachusetts Written Information Security Policies (WISP)
H. "Office of Inadequate Security" - DataBreaches.net