The Higher Learning Commission Action Project Directory

Northeast Iowa Community College

Project Details

Title	Information Security	**Status**	COMPLETED
Category	2-Accomplishing Other Distinctive Objectives	**Updated**	09-28-2012
Timeline		**Reviewed**	10-01-2012
Planned Project Kickoff	01-29-2011	**Created**	03-05-2012
Actual Completion	12-10-0012	**Version**	1

1: Project Goal

A: The goal of this Action Project is to create a systematic process of ongoing training and education of the college's information security program so that all employees will practice and model best practices for the protection of his/her identity as well as those they serve.

2: Reasons For Project

A: The Information Security Program was developed in response to the FTC's Red Flag Rules as set forth in the Fair and Accurate Credit Transactions Act (FACTA) of 2003. The protection of Confidential and Sensitive Information and the resources that support this is essential to the operations of the college. As information is shared, it is placed at risk for potential threats of employee errors, malicious or criminal actions, theft, and fraud. Such events could cause NICC to incur a loss of persons' confidential information, financial damages, fines, and penalties, and harm to the college's reputation.

3: Organizational Areas Affected

A: The organizational areas most affected by or involved in this Action Project includes: Business Services, Student Services, and Continuing Education. While other areas are impacted, these areas are assessed to be of greatest risk to a potential loss of confidential and sensitive information.

4: Key Organizational Process(es)

A: Organizational Processes expected to change:

1) Work area security and handling of information
2) Record retention and guidelines
3) Employee education and awareness
4) Use of electronic portable media

5: Project Time Frame Rationale

A: The Information Security Team was formed in late 2010 and given the task of developing and implementing measures to protect the privacy interests for the college. The first year of the action project focused on assessment of current processes and identification of vulnerabilities, assessment of resource needs, and providing a base training for college employees. Tasks accomplished include:

- ü Board of Trustee approval of the Information Security Program (December 2010).
- ü Assessment of current work processes and identification of risk areas
- ü Streamlining of policy and procedures for faxing, work area security
- ü Reviewed record retention guidelines with the resultant disposal of over 18,000 pounds of stored records
- ü Employee training to include identity theft, identified risk areas in the college, and maintaining a safe work area
- ü Requirement of signed confidentiality statements by all college personnel
- ü Identification of vendors who routinely use confidential information to conduct business with the college and the need to assess compliance with privacy and security policies of the industry and with NICC
- ü Overview by director of computer information services director to identify current practices in maintaining network security
- ü Development of guidelines for reported suspected breaches of privacy

ü Development of audits to be used in key college areas
ü Evaluated and purchased cross-cut shredders to dispose of confidential information
ü Evaluated and purchased privacy key pads for inputting of student ID and/or SSN numbers in open w ork areas
While these tasks have been initiated, the second year w ill focus on measuring the levels of compliance w ith recommend practices. Noted areas of deficiency w ill serve as the basis for continued employee education and training.

6: Project Success Monitoring

A: Monitoring w ill be completed by:

- Work area audits
- Human resource audit of new employee files
- Responses to questions/concerns by employee and staff through email questions, blogs, or other identified concerns
- Training evaluations

7: Project Outcome Measures

A: Target 1: Effective March 1, 2012 100% of new employees starting in March 2011 w ill be oriented to information security practices.

- Measure: ISO committee w ill develop orientation materials to be distributed by human resources to all department supervisors that outlines NICCs information security program and his/her responsibilities.
- Outcome: Effective March 1, 2012, 100% of new employee files w ill have signed confidentiality statements.
- Responsibility: Hiring supervisors, Human Resources
- Methodology: Audit of new hire files in human resources until 100% compliance is achieved and maintained for a period of one year.

Target 2: Effective January 1, 2011, Work area audits w ill be performed at scheduled intervals throughout the college. Performance benchmarks for compliance w ill be benchmarked at 80% for the first audit. Results w ill be analyzed to determine if benchmark level is met and w hat areas of training need further review. These benchmarks include compliance w ith w ork place safety as demonstrated by:

- Wearing of employee identification
- Placement and storage of personal items
- Proper methods of securing pc's w hen not in use
- Proper methods of storing CSI in w ork areas
- Proper use of spoken w ord w hen speaking w ith students/others about confidential information
- Securing of offices w hen not present on campus
- Proper methods of identity verification.
- Measure(s): Work Area Audit, Targeted Observation
- Outcome: 80% of observed/audited area w ill demonstrate compliance
- Responsibility: Audits w ill be conducted by assigned personnel in department/service areas.
- Methodology: Department/Service areas w ere ranked by risk by the ISO committee. Results w ill be summarized and analyzed by ISO team. After a period of one year, the audit cycle w ill be review ed and targeted to areas of greatest need for monitoring.

Project Update

1: Project Accomplishments and Status

A: The Information Security Team has instituted a systematic audit schedule. Audits for the first two quarters of the year were completed and results reviewed by the Team. Audits of new employee files indicate with compliance with reviewing and obtaining confidentiality agreements of new hires by supervisors. The process for identifying and reporting privacy concerns have improved as evidenced by communication to the security officer and filing of reports. New employee training is still under development. The project is on schedule and will be retired on December 29, 2012.

2: Institution Involvement

A: The primary areas of the college involved in implementation of this action project has been Business Services, Student Services, Computer Information Systems, Continuing Education (now known as Business and Community Solutions), Human Resources, and Administration. Committee membership is cross-disciplined and areas of greatest risk of identity theft loss play a primary role.
In the audit process, the team developed the audit form that reflected current college processes. Members of the team conduct the audits in designated areas and submit reports. The computer information systems staff conduct random "social engineering" exercises to identify needed areas of employee training in procedures. Persons on the committee are volunteered from their areas and/or have expressed interest in implementation of our processes.
The team meets monthly to identify concerns in department areas or expressed by staff and look for methods to improve processes.

3: Next Steps

A: The next steps will be to complete and analyze results from this year's work plan. The results are reported annually (December) to the Board of Trustees. Goals will be refined to meet the identified needs for 2013. By December, the Information Security Team will have a video of information security practices available for new employee orientation.

4: Resulting Effective Practices

A: The most effective practice resulting from this action project is the continued awareness that each employee is responsible for ensuring that confidential and sensitive information that they may work with must be protected from inadvertent or intentional loss. This awareness was enforced through the monitoring process (i.e. work area security practices, asking for and verification of identification at the work site or via telephone). The audit process is nonpunitive and is used to reinforce college processes and educate staff work area procedures. In departmental areas, staff take personal responsibility in doing things the "right way." For example, employees wearing required identification revealed a 92.5% compliance rate in the 2nd quarter of 2012 which is above the benchmark set by the team. Other areas of concern are addressed by supervisors. Effectiveness is demonstrated by meeting and exceeding the established thresholds for compliance in designated work areas. Effectiveness is also identified when concerns are reported to the security officer on possible threats or questionable practices on campus. Part of the audit process is asking when and how would you report a concern and ensuring staff know who to contact and what incidents may trigger an alert.

5: Project Challenges

A: The challenge we face will be the continuing need for education of new staff in our information security processes and then measuring the impact of the training. There is information on the cost of data breach to a company and the effectiveness of the training can only be a guesstimate of savings in reputation, time, and loss of a potential breach. Currently we have focused on the internal or "people" processes on campus since many breaches occur through unintentional human error. Network security is beyond the knowledge scope of the team and is dependent on the expertise of our computer information systems. They protect the network, we train the users in best practices. Our challenge will be to continue to be vigilant and alert on our practices.

Update Review

1: Project Accomplishments and Status

A: NEIowa Community College institution developed an action project to improve and monitor information security. In this case, information security is interpreted to mean the human elements of information management; aspects of information security that deal with IT and network security are not involved in the project. The project was developed in late 2010, and moved very quickly to achieve its earliest goals. During the first phase of the project (which was nearly all of 2011), the institution accomplished 12 distinct tasks that advanced

information security. Based on that momentum, the institution developed phase II of the project. The project has good accountability; it includes two major targets and each has clear measures, outcomes, person responsible and methodology through which the target will be achieved. Timing with which some goals are to be achieved is unclear. For example, the first bullet under Question 7 says that "Target 1: Effective March 1, 2012, 100% of new employees starting in March 2011 will be oriented …". It is not clear if that means it takes a year to achieve 100% compliance, or if one of those dates is incorrect. Other goals and timelines in Target 1 appear clear and actionable. Phase II of the action project appears to deal primarily with 2012, but Target 2 says "Effective January 2011, Work area audits will be performed …" The institution may wish to review the listed dates for Phase II to verify that all dates are consistent with their intent.

Phase II of the project occurred primarily in 2012 and this update addresses that phase. The Information Security Team has remained functional and has achieved many of the original goals. For example, the Team has completed an audit schedule and has two quarters of data in hand. The project design carried specific targets for compliance (e.g., 80-100% of employees will demonstrate specific behaviors). The update comments on completion of the audits, but does not identify percent compliance or other quantitative targets. If the Team is able to report such data, the project update might gain increased credibility with central administration. The update also states that "The project is on schedule and will be retired on December 29, 2012." However, Question 3 states that "…the goals are being refined to meet the identified needs for 2013." The Team may wish to make more clear which aspects of the information security program are project-based and which are sustainable changes that initiated in the project but continue after project completion.

2: Institution Involvement

A: The original project design identified three distinct units within the College that would be involved. Then project update identifies about six institutional units. It appears that the information security team has appropriately broadened its view of units that deal with secure information. Involvement of this wide a range of units is likely to increase people's awareness of information security issues, and likely to result in increased security for sensitive data (such as student records or financial information). The project update reports that " …computer information staff conduct random 'social engineering' exercises …" Because this project is so important to the like of the College, it seems that it would be useful to report on its progress to central administration. When such reporting occurs, the Information Security Team may wish to clarify the term "social engineering" to ensure there is no misunderstanding about its use.

3: Next Steps

A: The identified next steps for this action project center on a series of goals to be refined by December and to apply to the project (or its successor) in the following year. In fact, the institution reported earlier that the project ends in December 2012. However, some of the positive changes the Team has made should be sustained as permanent changes in institutional behavior (e.g., orientation and training information for new employees, carrying identification on campus). The Team may wish to clarify that the effort has been successful in identifying needs, developing a project to address those needs, and then using careful data analysis to ask which of those project activities should be sustained. Those sustainable goals might become the next steps at the conclusion of the action project.

4: Resulting Effective Practices

A: The institution has identified an effective practice that addresses care and management of sensitive data. It became clear through the project that not all individuals were aware of the risks of data mismanagement and the Team has developed practices the both increase awareness and guide proper data management. A strength that is apparent in the way this Team approached this issue is that compliance is monitored through an audit process but results of the audit are not punitive. As such, employees are more likely to share any learning that occurs from the audit process. The Team reports that the audit revealed a 92.5% compliance with the variable "employees wearing identification" during the second quarter of 2012. The Team may wish to expand on that reporting (i.e., report more variables and data for more than one quarter) because such data might demonstrate more clearly how successful the project has been. That more clear attribution of positive behavior to project input might make it easier to convince central administration to continue to support whatever activities the Team feels are necessary to sustain the positive changes.

5: Project Challenges

A: The project faces one central challenge: how to sustain the positive changes instituted to date. The project has achieved significant positive change. Individuals are more clearly identified on campus, data are more carefully handled (e.g., processing, storage, disposal all are more precisely and consistently handled). Much of that change has been achieved through training of staff at the College. As new staff join the College, or as new security practices are developed, there will be an ongoing need for such training. The Team identifies that training as a significant challenge. It is reasonable to expect that communicating about the project with central

administration would assist in overcoming that challenge. This information security project has reduced the risk that student data or institutional data will be mishandled or accidentally released. That higher level of accountability should be appealing to institutional officials who must take ultimate responsibility for data mismanagement, so increasing the security with which data are handled should be seen as being in everyone's best interests.

Project Outcome

1: **Reason for completion**

A: The goal of the action project was completed and a systematic process of ongoing information security training and education is in place.

2: **Success Factors**

A: An Information Security Team was established, roles were clearly defined, a systematic process of ongoing information security training and education is in place, and security practices have been implemented.

3: **Unsuccessful Factors**

A: The project faces one central challenge in how to sustain positive changes instituted and diligently train new staff.