Administrative Affairs Council
Conference Call Meeting Agenda
January 30, 2008 from 3-5 pm
Call 328-1620, access code 254160#

1. Review 2009-11 Biennial Budget Plans (McDonald)-to be sent under separate
cover

2. Review SBHE policy 1902-Emergency Notification Systems (Glatt/Seaworth)-
attached

3. Discuss Acquisition and Procedures for Imaging Systems (Thursby)-attached

4. Discuss Support of Third Party Software Systems (Thursby)-no attachment

5. Other

G:\laura\wpdocs\admin aff\agenda 013008
NORTH DAKOTA STATE BOARD OF HIGHER EDUCATION
POLICY MANUAL-DRAFT 1/9/08

SUBJECT: MISCELLANEOUS

Section: 1902 Emergency Notification Systems

1. Effective with the beginning of the fall 2008 semester, each institution and the NDUS office shall have in place an emergency notification system. An “emergency notification system” means a system established for the purpose of and dedicated to enabling institution or system officials to quickly contact or send messages to employees and students in event of an emergency. An “emergency” means a situation that poses an immediate threat to the health or safety of someone in the institution or system community or significantly disrupts institution or system programs and activities.

2. All NDUS employees, including student employees, shall participate in the emergency notification system. Participation means employees shall submit emergency notification information and update that information as provided in the institution’s or system’s emergency notification system policy and procedures.

3. Students other than student employees shall participate in the emergency notification system unless they “opt-out.” Students shall submit emergency notification information and have an opportunity to “opt-out” during registration or as otherwise provided under an institution’s emergency notification system policy or procedures.

4. Employee emergency notification telephone numbers or other emergency notification information is exempt from the state’s open records laws as provided in Policy1912 and may be released only as provided in that policy. Student emergency notification information, or contact information such as phone numbers or email addresses submitted for purposes of participation in an emergency notification system, shall be excluded from directory information and is therefore confidential as provided under the Family Educational Rights and Privacy Act (FERPA). However, if a student phone number or email or other address submitted for the purpose of participation in an emergency notification system is also contained in other institution records used for other purposes, the information contained in the other institution records is directory information and not confidential, unless a student has exercised the student’s right to refuse to permit disclosure of directory information.

5. Each institution shall adopt an emergency notification system policy and implementing procedures including:

   a. Statement that employee participation is mandatory;
   b. Provision for student participation and “opt-out;”
   c. Restrictions on use only for an emergency as defined in this policy and authorized tests, which must be conducted at least once each semester;
d. Policy governing student use of cell phones in class, including a provision permitting instructors to require students to turn cell phones off in class only if the instructor has a registered cell phone or other phone or other means of receiving emergency messages in use at all times students are required to turn their cell phones off;

e. Procedures governing updates and refreshing data, including a requirement that data be refreshed at least once each semester;

f. Identification of officials authorized to activate the system;

g. Instructions to employees and students for reporting emergency situations or incidents, including offices and telephone numbers of designated officials to whom emergency situations or incidents should be reported;

h. Guidelines regarding notice to or contacts with media;

i. Procedures for additional notifications as appropriate depending on circumstances.

6. Institution policy and procedures, including all updates or revisions, shall be filed with the system office.

7. The chancellor shall adopt an emergency notification procedure for the NDUS office, including a system for notifying office employees of an emergency specific to the office and for notifying key institution employees or designated institution emergency contacts as necessary or appropriate.

8. Subject to review and approval of the NDUS CIO, institutions may contract with a vendor or vendors for provision of emergency notification systems. If warranted based on consideration of administrative efficiencies and cost, the chancellor may require a single, uniform system for all institutions.

HISTORY: New Policy

REFERENCE:

W:\policies-procedures\1902 new 01.09.07.doc
Laura,

I have discussed with Rich his role in supporting a group you may appoint to look at the system procedure for the implementation and management of imaging systems. I would add the word acquisition as well when working on the procedure.

On Jan 17, 2008, at 9:30 AM, Laura Glatt wrote:

Admin. Affairs Council members: I would like to add this to our next agenda. Laura

------- Original Message -------

Subject: Re: imaging recommendation
Date: Thu, 17 Jan 2008 08:22:54 -0600
From: Darci Trenda <darci.trenda@ndus.nodak.edu>
Reply-To: darci.trenda@ndus.nodak.edu
Organization: North Dakota University System
To: laura.glatt@ndus.nodak.edu
References: <478E8A06.8000100@ndus.nodak.edu>

Imaging (finding 07-5)

Based on our review of campus departments that are using electronic imaging systems for e-file record retention, numerous internal controls, audit trail and system security issues were noted. For details by school and department please refer to Appendix A. The effects of these conditions range from loss of sensitive information to the web to potential loss of vital information on their systems without their knowledge to a possible catastrophic loss of information in the event of a critical system failure.

All computer systems must comply with SBHE 1901.2. In addition, to protect vital sensitive data, the institutions must apply strict and comprehensive internal controls. It is management’s responsibility to insure the safety, security, reliability and authenticity of the data placed on these systems.

Recommendation:

We recommend management ensure that:
Subject: Re: imaging recommendation  
From: Darci Trenda <darci.trenda@ndus.nodak.edu>  
Date: Thu, 17 Jan 2008 08:22:54 -0600  
To: laura.glatt@ndus.nodak.edu

**Imaging (finding 07-5)**

Based on our review of campus departments that are using electronic imaging systems for e-file record retention, numerous internal controls, audit trail and system security issues were noted. For details by school and department please refer to Appendix A. The effects of these conditions range from loss of sensitive information to the web to potential loss of vital information on their systems without their knowledge to a possible catastrophic loss of information in the event of a critical system failure.

All computer systems must comply with SBHE 1901.2. In addition, to protect vital sensitive data, the institutions must apply strict and comprehensive internal controls. It is management’s responsibility to insure the safety, security, reliability and authenticity of the data placed on these systems.

**Recommendation:**

We recommend management ensure that:

1. All imaging systems in use today and in the future are structured under a comprehensive internal control system to mitigate the potential loss or misuse of any information.

2. It assumes its role of designing, testing, and monitoring all computerized systems used by their institutions.

3. It assumes its role of establishing comprehensive policies and procedures to ensure proper internal controls and operating environments for imaging systems and source documents.

4. All imaging systems in use today and in the future comply with SBHE and other governmental policies.

**University System Response (Limit response to 100 words):**

Agree. Prior to the completion of FY09, the NDUS will develop a system procedure for the implementation and management of imaging systems.

Laura Glatt wrote:
Can you please send me just the information from the audit recommendations on imaging systems? Thanks, Laura

---

The North Dakota University System
is the Vital Link to a Brighter Future

Laura Glatt
Vice Chancellor for Administrative Affairs
North Dakota University System
600 East Boulevard Avenue, #215
Bismarck, ND 58505-0230
701.328.4116 phone
701.328.2961 fax
laura.glatt@ndus.nodak.edu

---

The North Dakota University System
is the Vital Link to a Brighter Future

Darci Trenda
Director of Financial Reporting
North Dakota University System
600 E Boulevard Ave Dept 215
Bismarck ND 58505-0230
701.328.3401

All recs Appendix A sent-3.doc

Content-Type: application/msword
Content-Encoding: base64
Appendix A - Imaging
Below is a listing of internal control and computer system problems identified in our review of the imaging systems used by the NDUS institutions. Although extensive, this listing is limited to our review and can not be considered complete.

NDUS – NDUS used three different imaging systems during fiscal year 2007. The systems used were Image Now (Registrar & Records, Grad School, Residents Life), Application Xtender (Financial Aid) and E-Cabinet (SLSC and HR/PR). Other departments on campus may be using these or other such systems, but the IT Department was not aware of any others, but not all such systems were being approved by the IT Department which is required by SBHE 1901.2. Each of these systems had significant internal control and record maintenance issues as described below:

1. Image Now:
   a. Registrar & Records Office: The records being e-stored by this office include, but not limited to, academic records, AP and similar test scores, college transcripts which include names, address, student number and SSN of the student FERPA consent to release forms, FERPA restricted directory and graduation lists.
      i. Source documents are only being verified by the individual assigned to scan the original document. This verification only consists of legibility – to see if the document can be read by the viewer. None of the document's contents is verified by a knowledgeable user nor is there a way for the system to document separate verification.
      ii. The individuals assigned to scan documents also have the ability to destroy any document on the system. Scanning personnel are usually part-time or student employees.
      iii. Audit software available on the system has not been enabled so no one has the ability to track system users or identify hackers.
      iv. Passwords are not required to be changed regularly and are not of a minimum length and are not required to use alpha, numeric or special keys.
      v. Back-up or restore systems have not been tested.
      vi. The software does not provide for ERM by providing automated deletion dates for the records stored or it has not been enabled.
      vii. There does not appear to be a system in place to monitor deletion dates for electronic records to comply with the institution’s record retention schedules.
      viii. Management has neglected to establish a system to comply with existing policies or to draft additional policies to ensure record maintenance, safety, authenticity to comply with HIPAA (Health Insurance Portability and Accountability Act).
      ix. A system for regular testing of system performance and reliability for hardware and software is not being performed or documented.
      x. The software has the ability to “lock-out” password/user ID’s who make repeated attempts to sign-on, but this software has not been enabled.
      xi. According to the Image Now permissions list, the “owner” has too much access to the system including the ability to destroy all system information.
      xii. The institution does not appear to have policies or procedures to regulate departmental implementation of imaging devices prior to obtaining appropriate authorization or attending classes on the proper use, access, security of the system being installed.
b. **Graduate School:** The records being imaged include, but are not limited to, teaching waiver requests, hiring form, change of funding form, financial certification form, tuition waivers, transcripts and resumes.
   i. Source documents are only being verified by the individual assigned to scan the original document. This verification only consists of legibility – to see if the document can be read by the viewer. None of the document's contents is verified by a knowledgeable user nor is there a way for the system to document separate verification.
   ii. The individuals assigned to scan documents also have the ability to destroy any document on the system. Scanning personnel are usually part-time or student employees.
   iii. Audit software available on the system has not been enabled so no one has the ability to track system users or identify hackers.
   iv. Passwords are not required to be changed regularly and are not of a minimum length and are not required to use alpha, numeric or special keys.
   v. Back-up or restore systems have not been tested.
   vi. The software does not provide for ERM by providing automated deletion dates for the records stored or it has not been enabled.
   vii. There does not appear to be a system in place to monitor deletion dates for electronic records to comply with the institution's record retention schedules.
   viii. Management has neglected to establish a system to comply with existing policies or to draft additional policies to ensure record maintenance, safety, authenticity to comply with HIPAA (Health Insurance Portability and Accountability Act).
   ix. A system for regular testing of system performance and reliability for hardware and software is not being performed or documented.
   x. The software has the ability to "lock-out" password/user ID's who make repeated attempts to sign-on, but this software has not been enabled.
   xi. According to the Image Now permissions list, the "owner" has too much access to the system including the ability to destroy all system information.
   xii. The institution does not appear to have policies or procedures to regulate departmental implementation of imaging devices prior to obtaining appropriate authorization or attending classes on the proper use, access, security of the system being installed.

c. **Residents Life:** The records being imaged include, but are not limited to, resident hall contracts, apartment contracts, criminal disclosure form, receipts and FERPA release forms.
   i. Source documents are only being verified by the individual assigned to scan the original document. This verification only consists of legibility – to see if the document can be read by the viewer. None of the document's contents is verified by a knowledgeable user nor is there a way for the system to document separate verification.
   ii. The individuals assigned to scan documents also have the ability to destroy any document on the system. Scanning personnel are usually part-time or student employees.
   iii. Audit software available on the system has not been enabled so no one has the ability to track system users or identify hackers.
   iv. Passwords are not required to be changed regularly and are not of a minimum length and are not required to use alpha, numeric or special keys.
   v. Back-up or restore systems have not been tested.
vi. The software does not provide for ERM by providing automated deletion dates for the records stored or it has not been enabled.

vii. There does not appear to be a system in place to monitor deletion dates for electronic records to comply with the institution's record retention schedules.

viii. Management has neglected to establish a system to comply with existing policies or to draft additional policies to ensure record maintenance, safety, authenticity to comply with HIPAA (Health Insurance Portability and Accountability Act).

ix. A system for regular testing of system performance and reliability for hardware and software is not being performed or documented.

x. The software has the ability to "lock-out" password/user ID's who make repeated attempts to sign-on, but this software has not been enabled.

xi. According to the Image Now permissions list, the "owner" has too much access to the system including the ability to destroy all system information.

xii. The institution does not appear to have policies or procedures to regulate departmental implementation of imaging devices prior to obtaining appropriate authorization or attending classes on the proper use, access, security of the system being installed.

2. Application Xtender (distributed by and maintained by Computer Services, Inc.)
   a. Financial Aid Office: The records being imaged by this office include, but not limited to, financial aid applications, student and parent tax documents and award letters.
      i. Source documents are only being verified by the individual assigned to scan the original document. This verification only consists of legibility – to see if the document can be read by the viewer. None of the document's contents is verified by a knowledgeable user nor is there a way for the system to document separate verification.
      ii. The individuals assigned to scan documents also have the ability to destroy any document on the system. Scanning personnel are usually part-time or student employees.
      iii. Current source documents are being destroyed within a month of being scanned, so no audit comparison could be done between the source and the imaged document for those older than a month.
      iv. Audit software available on the system has not been enabled so no one has the ability to track system users or identify hackers.
      v. Subsequent to our review, the audit software was enabled but no procedures exist for routine periodic review of the records.
      vi. Passwords are not required to be changed regularly and are not of a minimum length and are not required to use alpha, numeric or special keys.
      vii. Back-up or restore systems have not been tested.
      viii. The software does not provide for ERM by providing automated deletion dates for the records stored or it has not been enabled.
      ix. There does not appear to be a system in place to monitor deletion dates for electronic records to comply with the institution's record retention schedules.
      x. Management has neglected to establish a system to comply with existing policies or to draft additional policies to ensure record maintenance, safety, authenticity to comply with HIPAA (Health Insurance Portability and Accountability Act).
      xi. A system for regular testing of system performance and reliability for hardware and software is not being performed or documented.
xii. The software has the ability to “lock-out” password/user ID's who make repeated attempts to sign-on, but this software has not been enabled.

xiii. According to the Image Now permissions list, the “owner” has too much access to the system including the ability to destroy all system information.

xiv. The institution does not appear to have policies or procedures to regulate departmental implementation of imaging devices prior to obtaining appropriate authorization or attending classes on the proper use, access, security of the system being installed.

xv. The institution does not appear to have policies or procedures to ensure that the software used has the ability to be converted to other imaging systems if the manufacturer ceases to support it.

3. E-Cabinet:
   a. Student Loan Service Center: The documents being imaged by this department include, but are not limited to, student loan promissory notes, loan applications, loan cancellation and loan deferment waivers.
      i. This system was installed without the knowledge or approval of the IT department and when remodeling of the office where the server was located occurred, the server was moved and was reconnected to an unprotected web line which gave open web access to personal information.
      ii. This imaging system does not encrypt its stored information and is vulnerable to hacking.
      iii. Source documents are only being verified by the individual assigned to scan the original document. This verification only consists of legibility – to see if the document can be read by the viewer. None of the document's contents is verified by a knowledgeable user nor is there a way for the system to document separate verification.
      iv. The individuals assigned to scan documents also have the ability to destroy any document on the system. Scanning personnel are usually part-time or student employees.
      v. Current source documents are being destroyed within a month of being scanned, so no audit comparison could be done between the source and the imaged document for those older than a month.
      vi. Audit software available on the system has not been enabled so no one has the ability to track system users or identify hackers.
      vii. Subsequent to our review, the audit software was enabled but no procedures exist for routine periodic review of the records.
      viii. Passwords are not required to be changed regularly and are not of a minimum length and are not required to use alpha, numeric or special keys.
      ix. Back-up or restore systems have not been tested.
      x. The software does not provide for ERM by providing automated deletion dates for the records stored or it has not been enabled.
      xi. There does not appear to be a system in place to monitor deletion dates for electronic records to comply with the institution's record retention schedules.
      xii. Management has neglected to establish a system to comply with existing policies or to draft additional policies to ensure record maintenance, safety, authenticity to comply with HIPAA (Health Insurance Portability and Accountability Act).
      xiii. A system for regular testing of system performance and reliability for hardware and software is not being performed or documented.
xiv. The system does not appear to meet the compliance or certification requirements of DOD 5015.2.

xv. The software has the ability to “lock-out” password/user ID’s who make repeated attempts to sign-on, but this software has not been enabled.

xvi. According to the Image Now permissions list, the “owner” has too much access to the system including the ability to destroy all system information.

xvii. The institution does not appear to have policies or procedures to regulate departmental implementation of imaging devices prior to obtaining appropriate authorization or attending classes on the proper use, access, security of the system being installed.

xviii. The institution does not appear to have policies or procedures to ensure that the software used has the ability to be converted to other imaging systems if the manufacturer ceases to support it.

UND – UND used two different imaging systems during fiscal year 2007. The systems used were Image Now (Financial Aid, Registrar, Graduate School and Admissions & Records) and Application Xtender (Accounting Services, Payroll, Human Resources, Business Office, Purchasing and Housing). Other departments on campus may be using these or other such systems, but we are not aware of any others. Each of these systems had significant internal control and record maintenance issues as described below:

1. Image Now:
   a. Financial Aid Office: The records being imaged by this office include, but not limited to, financial aid applications, student and parent tax documents, checks and award letters.
      i. Source documents are only being verified by the individual assigned to scan the original document. This verification only consists of legibility – to see if the document can be read by the viewer. None of the document’s contents is verified by a knowledgeable user nor is there a way for the system to document separate verification.
      ii. The individuals assigned to scan documents also have the ability to destroy any document on the system. Scanning personnel are usually part-time or student employees.
      iii. During our test of expenses, we noted that source documents had been changed by Accounting Services and then scanned as original documents w/o apparent approval by the originating department.
      iv. Audit software available on the system has been enabled, but the log is not legible. So no one has the ability to track system users or identify hackers. Based on communications with UND, the manufacturer is working on this problem.
   b. No system or procedures exist for routine periodic review of the audit log.
   c. Source documents are only maintained for one month then they are destroyed. Without a system to verify electronic records to source documents, no assurance can be made that electronic records are accurate.
   d. Passwords are not required to be changed regularly and are not of a minimum length and are not required to use alpha, numeric or special keys.
   e. Back-up or restore systems have not been regularly tested.
   f. The software does not provide for ERM by providing automated deletion dates for the records stored or it has not been enabled.
NDUS
Planning and Administration
Appendix to 2007 Recommendations

x. There does not appear to be a system in place to monitor deletion dates for electronic records to comply with the institution’s record retention schedules.

xi. Management has neglected to establish a system to comply with existing policies or to draft additional policies to ensure record maintenance, safety, authenticity to comply with HIPAA (Health Insurance Portability and Accountability Act).

xii. A system for regular testing of system performance and reliability for hardware and software is not being performed or documented.

xiii. The software has the ability to “lock-out” password/user ID’s who make repeated attempts to sign-on, but this software has not been enabled.

xiv. According to the Image Now permissions list, the “owner” has too much access to the system including the ability to destroy all system information.

xv. The institution does not appear to have policies or procedures to regulate departmental implementation of imaging devices prior to obtaining appropriate authorization or attending classes on the proper use, access and security of the system being installed.

xvi. The institution does not appear to have policies or procedures to ensure that the software used has the ability to be converted to other imaging systems if the manufacturer ceases to support it.

b. Registrar’s Office: The records being e-stored by this office include, but not limited to, academic records, AP and similar test scores, college transcripts which include names, address, student number and SSN of the student FERPA consent to release forms, FERPA restricted directory and graduation lists.

i. Source documents are only being verified by the individual assigned to scan the original document. This verification only consists of legibility – to see if the document can be read by the viewer. None of the document’s contents is verified by a knowledgeable user nor is there a way for the system to document separate verification.

ii. The individuals assigned to scan documents also have the ability to destroy any document on the system. Scanning personnel are usually part-time or student employees.

iii. During our test of expenses, we noted that source documents had been changed by Accounting Services and then scanned as original documents w/o apparent approval by the originating department.

iv. Audit software available on the system has been enabled, but the log is not legible. So no one has the ability to track system users or identify hackers. Based on communications with UND, the manufacturer is working on this problem.

v. No system or procedures exist for routine periodic review of the audit log.

vi. Source documents are only maintained for one month then they are destroyed. Without a system to verify electronic records to source documents, no assurance can be made that electronic records are accurate.

vii. Passwords are not required to be changed regularly and are not of a minimum length and are not required to use alpha, numeric or special keys.

viii. Back-up or restore systems have not been regularly tested.

ix. The software does not provide for ERM by providing automated deletion dates for the records stored or it has not been enabled.

x. There does not appear to be a system in place to monitor deletion dates for electronic records to comply with the institution’s record retention schedules.
NDUS  
Planning and Administration  
Appendix to 2007 Recommendations

xi. Management has neglected to establish a system to comply with existing policies or to draft additional policies to ensure record maintenance, safety, authenticity to comply with HIPAA (Health Insurance Portability and Accountability Act).

xii. A system for regular testing of system performance and reliability for hardware and software is not being performed or documented.

xiii. The software has the ability to "lock-out" password/user ID's who make repeated attempts to sign-on, but this software has not been enabled.

xiv. According to the Image Now permissions list, the "owner" has too much access to the system including the ability to destroy all system information.

xv. The institution does not appear to have policies or procedures to regulate departmental implementation of imaging devices prior to obtaining appropriate authorization or attending classes on the proper use, access and security of the system being installed.

xvi. The institution does not appear to have policies or procedures to ensure that the software used has the ability to be converted to other imaging systems if the manufacturer ceases to support it.

c. Admissions & Records Office: The records being e-stored by this office include, but not limited to, academic records, AP and similiar test scores, college transcripts which include names, address, student number and SSN of the student FERPA consent to release forms, FERPA restricted directory and graduation lists.

i. Source documents are only being verified by the individual assigned to scan the original document. This verification only consists of legibility – to see if the document can be read by the viewer. None of the document's contents is verified by a knowledgeable user nor is there a way for the system to document separate verification.

ii. The individuals assigned to scan documents also have the ability to destroy any document on the system. Scanning personnel are usually part-time or student employees.

iii. Audit software available on the system has not been enabled so no one has the ability to track system users or identify hackers.

iv. Passwords are not required to be changed regularly and are not of a minimum length and are not required to use alpha, numeric or special keys.

v. Back-up or restore systems have not been tested.

vi. The software does not provide for ERM by providing automated deletion dates for the records stored or it has not been enabled.

vii. There does not appear to be a system in place to monitor deletion dates for electronic records to comply with the institution's record retention schedules

viii. Management has neglected to establish a system to comply with existing policies or to draft additional policies to ensure record maintenance, safety, authenticity to comply with HIPAA (Health Insurance Portability and Accountability Act).

ix. A system for regular testing of system performance and reliability for hardware and software is not being performed or documented.

x. The software has the ability to "lock-out" password/user ID's who make repeated attempts to sign-on, but this software has not been enabled.

xi. According to the Image Now permissions list, the "owner" has too much access to the system including the ability to destroy all system information.

xii. The institution does not appear to have policies or procedures to regulate departmental implementation of imaging devices prior to obtaining appropriate
authorization or attending classes on the proper use, access, security of the system being installed.

d. **Graduate School:** The records being e-stored by this office include, but not limited to, Graduate School E&R form, Dept recruitment request, job data hire form, position funding form, transcripts and test scores.

i. Source documents are only being verified by the individual assigned to scan the original document. This verification only consists of legibility – to see if the document can be read by the viewer. None of the document’s contents is verified by a knowledgeable user nor is there a way for the system to document separate verification.

ii. The individuals assigned to scan documents also have the ability to destroy any document on the system. Scanning personnel are usually part-time or student employees.

iii. During our test of expenses, we noted that source documents had been changed by Accounting Services and then scanned as original documents w/o apparent approval by the originating department.

iv. Audit software available on the system has been enabled, but the log is not legible. So no one has the ability to track system users or identify hackers. Based on communications with UND, the manufacturer is working on this problem.

v. No system or procedures exist for routine periodic review of the audit log.

vi. Source documents are only maintained for one month then they are destroyed. Without a system to verify electronic records to source documents, no assurance can be made that electronic records are accurate.

vii. Passwords are not required to be changed regularly and are not of a minimum length and are not required to use alpha, numeric or special keys.

viii. Back-up or restore systems have not been regularly tested.

ix. The software does not provide for ERM by providing automated deletion dates for the records stored or it has not been enabled.

x. There does not appear to be a system in place to monitor deletion dates for electronic records to comply with the institution’s record retention schedules

xi. Management has neglected to establish a system to comply with existing policies or to draft additional policies to ensure record maintenance, safety, authenticity to comply with HIPAA (Health Insurance Portability and Accountability Act).

xii. A system for regular testing of system performance and reliability for hardware and software is not being performed or documented.

xiii. The software has the ability to "lock-out" password/user ID’s who make repeated attempts to sign-on, but this software has not been enabled.

xiv. According to the Image Now permissions list, the "owner" has too much access to the system including the ability to destroy all system information.

xv. The institution does not appear to have policies or procedures to regulate departmental implementation of imaging devices prior to obtaining appropriate authorization or attending classes on the proper use, access and security of the system being installed.

xvi. The institution does not appear to have policies or procedures to ensure that the software used has the ability to be converted to other imaging systems if the manufacturer ceases to support it.
2. **Application Xtender:**
   a. **Accounting Services:** The records being e-stored by this office include, but not limited to, requests for payment, invoices, billings, refund/disbursements, vouchers, check copies, journal entries and other expense supporting documentation.
      i. Source documents are only being verified by the individual assigned to scan the original document. This verification only consists of legibility – to see if the document can be read by the viewer. None of the document’s contents is verified by a knowledgeable user nor is there a way for the system to document separate verification.
      ii. The individuals assigned to scan documents also have the ability to destroy any document on the system. Scanning personnel are usually part-time or student employees.
      iii. Current source documents are being destroyed within a month of being scanned, so no audit comparison could be done between the source and the imaged document for those older than a month.
      iv. Audit software available on the system has not been enabled so no one has the ability to track system users or identify hackers.
      v. Subsequent to our review, the audit software was enabled but no procedures exist for routine periodic review of the records.
      vi. Passwords are not required to be changed regularly and are not of a minimum length and are not required to use alpha, numeric or special keys.
      vii. Back-up or restore systems have not been tested.
      viii. The software does not provide for ERM by providing automated deletion dates for the records stored or it has not been enabled.
      ix. There does not appear to be a system in place to monitor deletion dates for electronic records to comply with the institution’s record retention schedules.
      x. Management has neglected to establish a system to comply with existing policies or to draft additional policies to ensure record maintenance, safety, authenticity to comply with HIPAA (Health Insurance Portability and Accountability Act).
      xi. A system for regular testing of system performance and reliability for hardware and software is not being performed or documented.
      xii. The software has the ability to “lock-out” password/user ID’s who make repeated attempts to sign-on, but this software has not been enabled.
      xiii. According to the Image Now permissions list, the “owner” has too much access to the system including the ability to destroy all system information.
      xiv. The institution does not appear to have policies or procedures to regulate departmental implementation of imaging devices prior to obtaining appropriate authorization or attending classes on the proper use, access, security of the system being installed.
      xv. The institution does not appear to have policies or procedures to ensure that the software used has the ability to be converted to other imaging systems if the manufacturer ceases to support it.

b. **Payroll:** The records being e-stored by this office include, but not limited to,
   i. Source documents are only being verified by the individual assigned to scan the original document. This verification only consists of legibility – to see if the document can be read by the viewer. None of the document’s contents is verified by a
knowledgeable user nor is there a way for the system to document separate verification.

ii. The individuals assigned to scan documents also have the ability to destroy any document on the system. Scanning personnel are usually part-time or student employees.

iii. Current source documents are being destroyed within a month of being scanned, so no audit comparison could be done between the source and the imaged document for those older than a month.

iv. Audit software available on the system has not been enabled so no one has the ability to track system users or identify hackers.

v. Subsequent to our review, the audit software was enabled but no procedures exist for routine periodic review of the records.

vi. Passwords are not required to be changed regularly and are not of a minimum length and are not required to use alpha, numeric or special keys.

vii. Back-up or restore systems have not been tested.

viii. The software does not provide for ERM by providing automated deletion dates for the records stored or it has not been enabled.

ix. There does not appear to be a system in place to monitor deletion dates for electronic records to comply with the institution’s record retention schedules.

x. Management has neglected to establish a system to comply with existing policies or to draft additional policies to ensure record maintenance, safety, authenticity to comply with HIPAA (Health Insurance Portability and Accountability Act).

xi. A system for regular testing of system performance and reliability for hardware and software is not being performed or documented.

xii. The software has the ability to “lock-out” password/user ID’s who make repeated attempts to sign-on, but this software has not been enabled.

xiii. According to the Image Now permissions list, the “owner” has too much access to the system including the ability to destroy all system information.

xiv. The institution does not appear to have policies or procedures to regulate departmental implementation of imaging devices prior to obtaining appropriate authorization or attending classes on the proper use, access, security of the system being installed.

xv. The institution does not appear to have policies or procedures to ensure that the software used has the ability to be converted to other imaging systems if the manufacturer ceases to support it.

c. **Human Resources:** The records being e-stored by this office include, but not limited to, personnel files, position appointments, salary and wage information, SSN, names and addresses.

i. Source documents are only being verified by the individual assigned to scan the original document. This verification only consists of legibility – to see if the document can be read by the viewer. None of the document’s contents is verified by a knowledgeable user nor is there a way for the system to document separate verification.

ii. The individuals assigned to scan documents also have the ability to destroy any document on the system. Scanning personnel are usually part-time or student employees.
iii. Current source documents are being destroyed within a month of being scanned, so no audit comparison could be done between the source and the imaged document for those older than a month.

iv. Audit software available on the system has not been enabled so no one has the ability to track system users or identify hackers.

v. Subsequent to our review, the audit software was enabled but no procedures exist for routine periodic review of the records.

vi. Passwords are not required to be changed regularly and are not of a minimum length and are not required to use alpha, numeric or special keys.

vii. Back-up or restore systems have not been tested.

viii. The software does not provide for ERM by providing automated deletion dates for the records stored or it has not been enabled.

ix. There does not appear to be a system in place to monitor deletion dates for electronic records to comply with the institution's record retention schedules.

x. Management has neglected to establish a system to comply with existing policies or to draft additional policies to ensure record maintenance, safety, authenticity to comply with HIPAA (Health Insurance Portability and Accountability Act).

xi. A system for regular testing of system performance and reliability for hardware and software is not being performed or documented.

xii. The software has the ability to "lock-out" password/user ID's who make repeated attempts to sign-on, but this software has not been enabled.

xiii. According to the Image Now permissions list, the "owner" has too much access to the system including the ability to destroy all system information.

xiv. The institution does not appear to have policies or procedures to regulate departmental implementation of imaging devices prior to obtaining appropriate authorization or attending classes on the proper use, access, security of the system being installed.

xv. The institution does not appear to have policies or procedures to ensure that the software used has the ability to be converted to other imaging systems if the manufacturer ceases to support it.

d. Business Office: The records being e-stored by this office include, but not limited to,

i. Source documents are only being verified by the individual assigned to scan the original document. This verification only consists of legibility – to see if the document can be read by the viewer. None of the document's contents is verified by a knowledgeable user nor is there a way for the system to document separate verification.

ii. The individuals assigned to scan documents also have the ability to destroy any document on the system. Scanning personnel are usually part-time or student employees.

iii. Current source documents are being destroyed within a month of being scanned, so no audit comparison could be done between the source and the imaged document for those older than a month.

iv. Audit software available on the system has not been enabled so no one has the ability to track system users or identify hackers.

v. Subsequent to our review, the audit software was enabled but no procedures exist for routine periodic review of the records.

vi. Passwords are not required to be changed regularly and are not of a minimum length and are not required to use alpha, numeric or special keys.
NDUS
Planning and Administration
Appendix to 2007 Recommendations

vii. Back-up or restore systems have not been tested.
viii. The software does not provide for ERM by providing automated deletion dates for the records stored or it has not been enabled.
ix. There does not appear to be a system in place to monitor deletion dates for electronic records to comply with the institution’s record retention schedules.
x. Management has neglected to establish a system to comply with existing policies or to draft additional policies to ensure record maintenance, safety, authenticity to comply with HIPAA (Health Insurance Portability and Accountability Act).
xi. A system for regular testing of system performance and reliability for hardware and software is not being performed or documented.
{xii. The software has the ability to “lock-out” password/user ID’s who make repeated attempts to sign-on, but this software has not been enabled.
{xiii. According to the Image Now permissions list, the “owner” has too much access to the system including the ability to destroy all system information.
{xiv. The institution does not appear to have policies or procedures to regulate departmental implementation of imaging devices prior to obtaining appropriate authorization or attending classes on the proper use, access, security of the system being installed.
xv. The institution does not appear to have policies or procedures to ensure that the software used has the ability to be converted to other imaging systems if the manufacturer ceases to support it.

e. Purchasing Office: The records being e-stored by this office include, but not limited to,

i. Source documents are only being verified by the individual assigned to scan the original document. This verification only consists of legibility – to see if the document can be read by the viewer. None of the document’s contents is verified by a knowledgeable user nor is there a way for the system to document separate verification.
ii. The individuals assigned to scan documents also have the ability to destroy any document on the system. Scanning personnel are usually part-time or student employees.
iii. Current source documents are being destroyed within a month of being scanned, so no audit comparison could be done between the source and the imaged document for those older than a month.
iv. Audit software available on the system has not been enabled so no one has the ability to track system users or identify hackers.
v. Subsequent to our review, the audit software was enabled but no procedures exist for routine periodic review of the records.
vi. Passwords are not required to be changed regularly and are not of a minimum length and are not required to use alpha, numeric or special keys.
vii. Back-up or restore systems have not been tested.
viii. The software does not provide for ERM by providing automated deletion dates for the records stored or it has not been enabled.
ix. There does not appear to be a system in place to monitor deletion dates for electronic records to comply with the institution’s record retention schedules.
x. Management has neglected to establish a system to comply with existing policies or to draft additional policies to ensure record maintenance, safety, authenticity to comply with HIPAA (Health Insurance Portability and Accountability Act).
xi. A system for regular testing of system performance and reliability for hardware and software is not being performed or documented.

xii. The software has the ability to "lock-out" password/user ID's who make repeated attempts to sign-on, but this software has not been enabled.

xiii. According to the Image Now permissions list, the "owner" has too much access to the system including the ability to destroy all system information.

xiv. The institution does not appear to have policies or procedures to regulate departmental implementation of imaging devices prior to obtaining appropriate authorization or attending classes on the proper use, access, security of the system being installed.

xv. The institution does not appear to have policies or procedures to ensure that the software used has the ability to be converted to other imaging systems if the manufacturer ceases to support it.

f. **Housing Office:** The records being e-stored by this office include, but not limited to,

i. Source documents are only being verified by the individual assigned to scan the original document. This verification only consists of legibility – to see if the document can be read by the viewer. None of the document's contents is verified by a knowledgeable user nor is there a way for the system to document separate verification.

ii. The individuals assigned to scan documents also have the ability to destroy any document on the system. Scanning personnel are usually part-time or student employees.

iii. Current source documents are being destroyed within a month of being scanned, so no audit comparison could be done between the source and the imaged document for those older than a month.

iv. Audit software available on the system has not been enabled so no one has the ability to track system users or identify hackers.

v. Subsequent to our review, the audit software was enabled but no procedures exist for routine periodic review of the records.

vi. Passwords are not required to be changed regularly and are not of a minimum length and are not required to use alpha, numeric or special keys.

vii. Back-up or restore systems have not been tested.

viii. The software does not provide for ERM by providing automated deletion dates for the records stored or it has not been enabled.

ix. There does not appear to be a system in place to monitor deletion dates for electronic records to comply with the institution's record retention schedules

x. Management has neglected to establish a system to comply with existing policies or to draft additional policies to ensure record maintenance, safety, authenticity to comply with HIPAA (Health Insurance Portability and Accountability Act).

xi. A system for regular testing of system performance and reliability for hardware and software is not being performed or documented.

xii. The software has the ability to "lock-out" password/user ID's who make repeated attempts to sign-on, but this software has not been enabled.

xiii. According to the Image Now permissions list, the "owner" has too much access to the system including the ability to destroy all system information.

xiv. The institution does not appear to have policies or procedures to regulate departmental implementation of imaging devices prior to obtaining appropriate
MISU — MISU uses the Image Now software for imaging Financial Aid, Registrar and Admissions Office records. Other departments on campus may be using this or other such systems, but we are not aware of any others. Based on our review we noted this system had significant internal control and record maintenance issues as described below:

1. Image Now:
   a. Financial Aid Office: The records being imaged by this office include, but not limited to, financial aid applications, appeals, special circumstance issues, student and parent tax documents, checks and award letters.
      i. Source documents are only being verified by the individual assigned to scan the original document. This verification only consists of legibility – to see if the document can be read by the viewer. None of the document's contents is verified by a knowledgeable user nor is there a way for the system to document separate verification.
      ii. The individuals assigned to scan documents also have the ability to destroy any document on the system. Scanning personnel are usually part-time or student employees.
      iii. Audit software available on the system has been enabled, but the log is not legible. So no one has the ability to track system users or identify hackers.
      iv. No system or procedures exist for routine periodic review of the audit log.
      v. Source documents are only maintained for one month then they are destroyed. Without a system to verify electronic records to source documents, no assurance can be made that electronic records are accurate.
      vi. Passwords are not required to be changed regularly and are not of a minimum length and are not required to use alpha, numeric or special keys.
      vii. Back-up or restore systems have not been regularly tested.
      viii. The software does not provide for ERM by providing automated deletion dates for the records stored or it has not been enabled.
      ix. There does not appear to be a system in place to monitor deletion dates for electronic records to comply with the institution's record retention schedules
      x. Management has neglected to establish a system to comply with existing policies or to draft additional policies to ensure record maintenance, safety, authenticity to comply with HIPAA (Health Insurance Portability and Accountability Act).
      xi. A system for regular testing of system performance and reliability for hardware and software is not being performed or documented.
      xii. The software has the ability to "lock-out" password/user ID's who make repeated attempts to sign-on, but this software has not been enabled.
      xiii. According to the Image Now permissions list, the "owner" has too much access to the system including the ability to destroy all system information.
xiv. The institution does not appear to have policies or procedures to regulate departmental implementation of imaging devices prior to obtaining appropriate authorization or attending classes on the proper use, access and security of the system being installed.

xv. The institution does not appear to have policies or procedures to ensure that the software used has the ability to be converted to other imaging systems if the manufacturer ceases to support it.

b. Registrar's Office: The records being imaged by this office include, but not limited to, Student files, transcripts, grade changes, name changes, add/drop requests and sometimes SSN.

i. Source documents are only being verified by the individual assigned to scan the original document. This verification only consists of legibility – to see if the document can be read by the viewer. None of the document’s contents is verified by a knowledgeable user nor is there a way for the system to document separate verification.

ii. The individuals assigned to scan documents also have the ability to destroy any document on the system. Scanning personnel are usually part-time or student employees.

iii. Audit software available on the system has been enabled, but the log is not legible. So no one has the ability to track system users or identify hackers.

iv. No system or procedures exist for routine periodic review of the audit log.

v. Source documents are maintained for one year and then they are destroyed. However, within this one year period, source documents are not compared to imaged documents to assure validity.

vi. Passwords are not required to be changed regularly and are not of a minimum length and are not required to use alpha, numeric or special keys.

vii. Back-up or restore systems have not been regularly tested.

viii. The software does not provide for ERM by providing automated deletion dates for the records stored or it has not been enabled.

ix. There does not appear to be a system in place to monitor deletion dates for electronic records to comply with the institution's record retention schedules.

x. Management has neglected to establish a system to comply with existing policies or to draft additional policies to ensure record maintenance, safety, authenticity or to comply with HIPAA (Health Insurance Portability and Accountability Act) rules.

xi. A system for regular testing of system performance and reliability for hardware and software is not being performed or documented.

xii. The software has the ability to "lock-out" password/user ID's who make repeated attempts to sign-on, but this software has not been enabled.

xiii. According to the Image Now permissions list, the "owner" has too much access to the system including the ability to destroy all system information.

xiv. The institution does not appear to have policies or procedures to regulate departmental implementation of imaging devices prior to obtaining appropriate authorization or attending classes on the proper use, access and security of the system being installed.

xv. The institution does not appear to have policies or procedures to ensure that the software used has the ability to be converted to other imaging systems if the manufacturer ceases to support it.
c. **Admissions Office:** The records being imaged by this office include, but not limited to, Applications, ACT & SAT scores, HS & college transcripts, admissions letters.

   i. Source documents are only being verified by the individual assigned to scan the original document. This verification only consists of legibility – to see if the document can be read by the viewer. None of the document’s contents is verified by a knowledgeable user nor is there a way for the system to document separate verification.

   ii. Audit software available on the system has been enabled, but the log is not legible. So no one has the ability to track system users or identify hackers.

   iii. No system or procedures exist for routine periodic review of the audit log.

   iv. Passwords are not required to be changed regularly and are not of a minimum length and are not required to use alpha, numeric or special keys.

   v. Back-up or restore systems have not been regularly tested.

   vi. The software does not provide for ERM by providing automated deletion dates for the records stored or it has not been enabled.

   vii. There does not appear to be a system in place to monitor deletion dates for electronic records to comply with the institution’s record retention schedules

   viii. Management has neglected to establish a system to comply with existing policies or to draft additional policies to ensure record maintenance, safety, authenticity to comply with HIPAA (Health Insurance Portability and Accountability Act).

   ix. A system for regular testing of system performance and reliability for hardware and software is not being performed or documented.

   x. The software has the ability to “lock-out” password/user ID’s who make repeated attempts to sign-on, but this software has not been enabled.

   xi. According to the Image Now permissions list, the “owner” has too much access to the system including the ability to destroy all system information.

   xii. The institution does not appear to have policies or procedures to regulate departmental implementation of imaging devices prior to obtaining appropriate authorization or attending classes on the proper use, access and security of the system being installed.

   xiii. The institution does not appear to have policies or procedures to ensure that the software used has the ability to be converted to other imaging systems if the manufacturer ceases to support it.

**BSC – BSC uses the Image Now software for imaging Financial Aid, Registrar and Admissions Office records. Other departments on campus may be using this or other such systems, but we are not aware of any others. Based on our review we noted this system had significant internal control and record maintenance issues as described below:**

1. **Image Now:**
   a. **Financial Aid Office:** The records being imaged by this office include, but not limited to, financial aid applications, appeals, special circumstance issues, student and parent tax documents, checks and award letters.

   i. Source documents are only being verified by the individual assigned to scan the original document. This verification only consists of legibility – to see if the document can be read by the viewer. None of the document’s contents is verified by a
knowledgeable user nor is there a way for the system to document separate verification.
ii. The individuals assigned to scan documents also have the ability to destroy any document on the system. Scanning personnel are usually part-time or student employees.
iii. Audit software available on the system has not been enabled. So no one has the ability to track system users or identify hackers.
iv. No system or procedures exist for routine periodic review of the audit log.
v. Source documents are only maintained for one month then they are destroyed. Without a system to verify electronic records to source documents, no assurance can be made that electronic records are accurate.
vi. Back-up or restore systems have not been regularly tested.
vii. The software does not provide for ERM by providing automated deletion dates for the records stored or it has not been enabled.
viii. There does not appear to be a system in place to monitor deletion dates for electronic records to comply with the institution’s record retention schedules
ix. Management has neglected to establish a system to comply with existing policies or to draft additional policies to ensure record maintenance, safety, authenticity to comply with HIPAA (Health Insurance Portability and Accountability Act).
x. A system for regular testing of system performance and reliability for hardware and software is not being performed or documented.
xii. According to the Image Now permissions list, the “owner” has too much access to the system including the ability to destroy all system information.
x. The institution does not appear to have policies or procedures to regulate departmental implementation of imaging devices prior to obtaining appropriate authorization or attending classes on the proper use, access and security of the system being installed.
xiii. The institution does not appear to have policies or procedures to ensure that the software used has the ability to be converted to other imaging systems if the manufacturer ceases to support it.

b. Registrar's Office: The records being imaged by this office include, but not limited to, Student files, HS and college transcripts, applications, ACT tests, placement, grade changes, name changes, add/drop requests and sometimes SSN. Tom Leno 224-5497

i. Source documents are only being verified by the individual assigned to scan the original document. This verification only consists of legibility – to see if the document can be read by the viewer. None of the document’s contents is verified by a knowledgeable user nor is there a way for the system to document separate verification.
ii. The individuals assigned to scan documents also have the ability to destroy any document on the system. Scanning personnel are usually part-time or student employees.
iii. Audit software available on the system has not been enabled. So no one has the ability to track system users or identify hackers.
iv. No system or procedures exist for routine periodic review of the audit log.
v. Source documents are maintained for two years and then they are destroyed. However, within this period, source documents are not compared to imaged documents to assure validity.
vi. Back-up or restore systems have not been regularly tested.
vii. The software does not provide for ERM by providing automated deletion dates for the records stored or it has not been enabled.

viii. There does not appear to be a system in place to monitor deletion dates for electronic records to comply with the institution’s record retention schedules.

ix. Management has neglected to establish a system to comply with existing policies or to draft additional policies to ensure record maintenance, safety, authenticity or to comply with HIPAA (Health Insurance Portability and Accountability Act) rules.

x. A system for regular testing of system performance and reliability for hardware and software is not being performed or documented.

xi. According to the Image Now permissions list, the “owner” has too much access to the system including the ability to destroy all system information.

xii. The institution does not appear to have policies or procedures to regulate departmental implementation of imaging devices prior to obtaining appropriate authorization or attending classes on the proper use, access and security of the system being installed.

xiii. The institution does not appear to have policies or procedures to ensure that the software used has the ability to be converted to other imaging systems if the manufacturer ceases to support it.

c. **Admissions Office:** The records being imaged by this office include, but not limited to, students admissions file, application, immunization, HS and college transcripts, ACT scores and student correspondence. Per discussion with Carla Gabrial (Dean) 224-5426, the imaging system is only accessed through the school’s LAN which requires 8 character passwords and password changes every 90 days. Carol Flaa 224-5519.

i. Source documents are only being verified by the individual assigned to scan the original document. This verification only consists of legibility – to see if the document can be read by the viewer. None of the document's contents is verified by a knowledgeable user nor is there a way for the system to document separate verification.

ii. The individuals assigned to scan documents also have the ability to destroy any document on the system. Scanning personnel are usually part-time or student employees.

iii. Audit software available on the system has not been enabled. So no one has the ability to track system users or identify hackers.

iv. No system or procedures exist for routine periodic review of the audit log.

v. Source documents are maintained for two years and then they are destroyed. However, within this period, source documents are not compared to imaged documents to assure validity.

vi. Back-up or restore systems have not been regularly tested.

vii. The software does not provide for ERM by providing automated deletion dates for the records stored or it has not been enabled.

viii. There does not appear to be a system in place to monitor deletion dates for electronic records to comply with the institution’s record retention schedules.

ix. Management has neglected to establish a system to comply with existing policies or to draft additional policies to ensure record maintenance, safety, authenticity or to comply with HIPAA (Health Insurance Portability and Accountability Act).

x. A system for regular testing of system performance and reliability for hardware and software is not being performed or documented.
According to the Image Now permissions list, the "owner" has too much access to the system including the ability to destroy all system information.

The institution does not appear to have policies or procedures to regulate departmental implementation of imaging devices prior to obtaining appropriate authorization or attending classes on the proper use, access and security of the system being installed.

The institution does not appear to have policies or procedures to ensure that the software used has the ability to be converted to other imaging systems if the manufacturer ceases to support it.

NDSCS — NDSCS uses the Image Now imaging software for the. Other departments on campus may be using this or other such systems, but we are not aware of any others. Based on our review we noted this system had significant internal control and record maintenance issues as described below:

1. **Image Now:**
   a. **Enrollment Services:** The records being imaged by this office include, but not limited to, students admissions file, application, immunization, HS and college transcripts, ACT scores and student correspondence.

   i. Source documents are only being verified by the individual assigned to scan the original document. This verification only consists of legibility — to see if the document can be read by the viewer. None of the document’s contents is verified by a knowledgeable user nor is there a way for the system to document separate verification.

   ii. The individuals assigned to scan documents also have the ability to destroy any document on the system. Scanning personnel are usually part-time or student employees.

   iii. Audit software available on the system has been enabled, but the log is not legible. So no one has the ability to track system users or identify hackers.

   iv. No system or procedures exist for routine periodic review of the audit log.

   v. Back-up or restore systems have not been regularly tested.

   vi. Back-up media is stored in the IT area, not off site.

   vii. The software does not provide for ERM by providing automated deletion dates for the records stored or it has not been enabled.

   viii. There does not appear to be a system in place to monitor deletion dates for electronic records to comply with the institution’s record retention schedules

   ix. Management has neglected to establish a system to comply with existing policies or to draft additional policies to ensure record maintenance, safety, authenticity to comply with HIPAA (Health Insurance Portability and Accountability Act).

   x. Passwords are not required to be changed regularly.

   xi. A system for regular testing of system performance and reliability for hardware and software is not being performed or documented.

   xii. According to the Image Now permissions list, the “owner” has too much access to the system including the ability to destroy all system information.

   xiii. The institution does not appear to have policies or procedures to regulate departmental implementation of imaging devices prior to obtaining appropriate authorization or attending classes on the proper use, access and security of the system being installed.
xiv. The institution does not appear to have policies or procedures to ensure that the software used has the ability to be converted to other imaging systems if the manufacturer ceases to support it.
b. **Human Resources:** The records being imaged by this office include, but not limited to, personnel files, position appointments, salary and wage information, SSN, names and addresses.
   
i. Source documents are only being verified by the individual assigned to scan the original document. This verification only consists of legibility – to see if the document can be read by the viewer. None of the document’s contents is verified by a knowledgeable user nor is there a way for the system to document separate verification.
   ii. The individuals assigned to scan documents also have the ability to destroy any document on the system. Scanning personnel are usually part-time or student employees.
   iii. Current source documents are being destroyed within a month of being scanned, so no audit comparison could be done between the source and the imaged document for those older than a month.
   iv. Audit software available on the system has not been enabled so no one has the ability to track system users or identify hackers.
   v. Subsequent to our review, the audit software was enabled but no procedures exist for routine periodic review of the records.
   vi. Passwords are not required to be changed regularly.
   vii. Back-up or restore systems have not been tested.
   viii. Back-up media is stored in the IT area, not off site.
   ix. The software does not provide for ERM by providing automated deletion dates for the records stored or it has not been enabled.
   x. There does not appear to be a system in place to monitor deletion dates for electronic records to comply with the institution’s record retention schedules.
   xi. Management has neglected to establish a system to comply with existing policies or to draft additional policies to ensure record maintenance, safety, authenticity to comply with HIPAA (Health Insurance Portability and Accountability Act).
   xii. A system for regular testing of system performance and reliability for hardware and software is not being performed or documented.
   xiii. According to the Image Now permissions list, the “owner” has too much access to the system including the ability to destroy all system information.
   xiv. The institution does not appear to have policies or procedures to regulate departmental implementation of imaging devices prior to obtaining appropriate authorization or attending classes on the proper use, access, security of the system being installed.
   xv. The institution does not appear to have policies or procedures to ensure that the software used has the ability to be converted to other imaging systems if the manufacturer ceases to support it.

**VCSU** – VCSU uses an off-the-shelf scanner to electronically image its paper copies. The documents are stored on files on a local server housed in the IT server area. Other departments on campus may be using this or other such systems, but we are not aware of any others. Based on our review we noted this system had significant internal control and record maintenance issues as described below:
1. **Blackboard Academic Suite**

   a. **Financial Aid Office:** The records being imaged by this office include, but not limited to, financial aid applications, appeals, special circumstance issues, student and parent tax documents, checks and award letters.

      i. Blackboard is an e-file imaging software, not an e-record software. As such, the document scanned can be altered.

      ii. Source documents are only being verified by the individual assigned to scan the original document. This verification only consists of legibility – to see if the document can be read by the viewer. All of the financial aid staff can scan, save and destroy any imaged document.

      iii. Pass-words are not “locked out” if entered multiple times.

      iv. Current source documents are being destroyed within a month of being scanned, so no audit comparison could be done between the source and the imaged document for those older than a month.

      v. Audit software available on the system has not been enabled so no one has the ability to track system users or identify hackers.

      vi. Passwords are not required to be changed regularly.

      vii. The server does not have anti-virus software, however the server is masked behind the ITS fire-wall.

      viii. The software does not provide for ERM by providing automated deletion dates for the records stored or it has not been enabled.

      ix. There does not appear to be a system in place to monitor deletion dates for electronic records to comply with the institution’s record retention schedules

      x. Management has neglected to establish a system to comply with existing policies or to draft additional policies to ensure record maintenance, safety, authenticity to comply with HIPAA (Health Insurance Portability and Accountability Act).

      xi. A system for regular testing of system performance and reliability for hardware and software is not being performed or documented.

      xii. The institution does not appear to have policies or procedures to regulate departmental implementation of imaging devices prior to obtaining appropriate authorization or attending classes on the proper use, access, security of the system being installed.

      xiii. The institution does not appear to have policies or procedures to ensure that the software used has the ability to be converted to other imaging systems if the manufacturer ceases to support it.