ABC College

Date: August 30, 2008
CIO: Mary Johnson, mjohnson@abc.edu
CISO: Joe Smith, jsmith@abc.edu

Risk 1: Storing student records on laptops

Responsible Contact: John Doe, jdoe@abc.edu, IT security engineer

Risk statement: The risk that student records stored on laptops could be exposed to unauthorized individuals is significant because laptops are easily lost or stolen. Depending on the number of student records exposed, notifications and associated expenses could be very high. Media attention resulting from student record exposures would negatively impact the reputation of ABC College, which could result in reduced enrollment, donations and other funding.

Mitigation:

- Policies and procedures will be implemented to minimize the number individuals authorized to store student records on laptops.
- For those laptops authorized to store student records, whole-disk encryption will be required.
- End-users will be taught encryption procedures.

Schedule:

• Enact encryption policies and procedures:	October 30, 2008
• Build key management server:	October 30, 2008
• Train users:	December 15, 2008
• Implement encryption:	December 15, 2008

Resources

• Encryption software	$5000.00
• Key management server	$2000.00
• 0.25 FTE	Use existing staff

Metrics

- End-users will be quizzed before and after training to evaluate the improvement of their data protection skills.
- Laptops used to store student records will be audited before and after encryption is implemented to evaluate data protection improvement.
- Laptop security incident number and severity for one year prior to the policy implementation will be evaluated and compared to incidents during the year after the policy implementation.

Risk 2: Using student records on unmanaged computers

Responsible Contact: John Doe, jdoe@abc.edu, IT security engineer

Risk statement: The risk of storing student records on computers that are not managed by professional ABC College IT staff is significant because computers that are not professionally managed are more likely to be non-compliant with ABC college security policies. Depending on the number of student records exposed, notifications and associated expenses could be very high. Media attention resulting from student record exposures would negatively impact the reputation of ABC College, which could result in reduced enrollment, donations and other funding.

Mitigation: A policy will be implemented to prohibit the use of student records on computers that are not managed by profession ABC College IT staff. The Sr. Vice President of Student Affairs must authorize and document any exceptions to this policy. Where exceptions can't be avoided, minimum security requirements will be documented and periodically verified. Authorized exceptions will be periodically audited

Schedule:

- Enact policy: October 30, 2008
- Document exceptions: October 30, 2008
- Enforce minimum security requirements: October 30, 2008

Resources: Existing staff can be used since only about 0.25 FTE is needed. No equipment is needed since existing equipment can be used.

Metrics

- The number of unmanaged computers used with student records will be counted before and after implementation of the new policy.
- The security status of unmanaged computers used with student records will be evaluated before and after implementation of the new policy.
- Authorization records will be audited one year after implementation of the policy to ensure that exceptions are limited to those with no alternative.

Risk 3: Disposal of media containing student records

Responsible Contact: John Doe, jdoe@abc.edu, IT security engineer

Risk statement: The risk that student records might be exposure to unauthorized individuals is high if the media upon which they are stored is not rendered unrecoverable prior to disposal. Depending on the number of student records exposed, notifications and associated expenses could be very high. Media attention resulting from student record exposures would negatively impact the reputation of ABC College, which could result in reduced enrollment, donations and other funding.

Mitigation:

- Policies and procedures will be implemented to render unrecoverable any media used to store student records prior to disposal.
- An agreement will be negotiated with a certified media disposal contractor.
- Relevant staff will be trained about disposal procedures.

Schedule:

- Implement disposal policy and procedures: October 30, 2008
- Train staff: December 15, 2008
- Implement encryption: December 15, 2008

Resources

• Disposal contract	$5000.00
• 0.25 FTE	Use existing staff

Metrics

- Relevant staff will be surveyed before and after implementation to the new policy to evaluate the improvement in disposal procedures.
- Media destined for disposal will be sampled and tested for recoverability to evaluate compliance with the new policy.

The above mitigations are appropriate to the risks. Adequate budget will be provided to implement these mitigations.

X ______________________________

Mary Johnson
Chief Information Officer

X ______________________________

Joe Smith
Chief Information Security Officer