	Title: Secure Retention of Students Records	POL-314 Revision # 0.0
Prepared By:	Patricia Cueva, Registrar	Date Prepared: 10/16/2015
Approved By:	College President's Signature	Date Approved: 12/09/2015
Effective Date: 12/09/2015	Board of Trustees President's Signature	Date Approved: 12/09/2015

314.1 POLICY STATEMENT

NWIC adheres to and fully supports the legislation and regulations of the Family Educational Rights and Privacy Act (FERPA) of 1974. The Registrar, located in Enrollment Services, is NWIC's FERPA liaison and records custodian. Information regarding FERPA, records confidentiality, access to student information, and directory information is clearly laid out in the college catalog and current NWIC Student Handbook. Students may request their directory information to be restricted, which is flagged electronically in the student management system.

The Student Management System and related databases reside on a dedicated server with a next day service agreement. The server is configured with redundant storage, processors, memory, and power, to reduce the impact of single-component failure.

314.2 PURPOSE

The purpose of this policy is to ensure the security, availability, and retention of all student records received. The policy is meant to protect the interests of both students and employees of the College.

314.3 SCOPE

This policy applies to all electronic records contained in the Student Management System, which includes all students.

314.4 RESPONSIBILITY

It is the responsibility of the FERPA liaison and records custodian to ensure confidentiality of academic records. The Information Systems Department is responsible for the electronic storage, back-up, and security of the servers in which the data is stored.

314.5 DEFINITIONS

The term "record" means all documents (written or electronic) created, produced, received, or maintained by any staff on behalf of the college.

314.6 PROCEDURE

Disk-to-disk backups of all databases are taken daily and resynchronized every fifteen minutes. Daily backups are retained for thirty days. Native backups are also taken for redundancy, and retained for thirty or more days as space permits. On the first weekday of each month, several backups are copied to physical medium and moved to a secured offsite location. All databases are stored on self-encrypting disks.

Information other than official student and financial records (file system storage) resides on a separate server with a next day service agreement. This server is configured with redundant storage, processors, memory, and power, to reduce the impact of single-component failure. Disk-to-disk backups of relevant files are taken daily and resynchronized every fifteen minutes. Daily backups are retained for thirty days. Access to any electronic records is password-protected.

All servers are housed in a windowless room with a single inside door and a high security lock. The premises is monitored by surveillance cameras and secured with an alarm system that notifies local authorities in the event of a breech. The room contains halon fire suppression, redundant air conditioning, and redundant power circuits with both uninterruptable power supplies at each receptacle and generator backup.

314.7 REVIEW DATE

Reviewed every 3 years.