

Information Technology Data Security and Recovery Process

The following text describes the security and recovery processes that are currently implemented by the Northwest Indian College Information Services department.

The Student Information 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. Disk-to-disk backups of all databases are taken daily and resynchronized every fifteen minutes. Daily backups are retained for thirty days, and housed in a separate building from the production servers. 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 native 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, and housed in a separate building from the production servers.

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