Policy & Procedure No. 7.006

Nunez Community College

Title: Identity Theft Prevention and Database Breach Notification Policy

Effective Date: 11-9-2018

Last Revision Date: 2015
Cancellation:

Department/Office: Information Technology

PURPOSE

This policy has been created to keep Nunez compliant with Louisiana Database Breach Notification Law SB205 Act 409. This policy will describe the defenses that are utilized in order to prevent identity theft at Nunez community college in addition to describing the procedure for notifying affected individuals in the event of a database breach.

SCOPE

This policy applies to full-time employees, part-time employees and interns (student workers).

POLICY

Infrastructure Protection:

Nunez Community college employs a number of hardware and software suites in order to prevent identity theft. The entire infrastructure is first guarded by 3 routers which contain several anti-hacking protocols to prevent authorized users from hacking into the network from the World Wide Web (www). The first router is maintained by the networking staff at Louisiana Optical Network Initiative (LONI) which provides the college with its internet connection and subsequent routing to LCTCS servers for the purposes of Banner activities. The 2nd and 3rd routers are both housed on campus; the 2nd router was provided by the LCTCS and allows for secure connection to Banner while the 3rd router is owned and maintained by Nunez Community College IT staff. The 2nd and 3rd routers have policies in place that prevent anyone from outside of the campus from gaining access to the infrastructure; the only "conduit" to the outside is a password guarded VPN which is only utilized by IT staff for the purposes of conducting maintenance when not on campus during off peak hours. The 3rd router, as well as all networking switches in place across campus, are linked with network monitoring software, currently Extreme's NetSight Console, that provide IT staff

the ability to monitor network traffic and will warn staff if there is any unusual activity which is investigated by IT staff.

Beyond the switches and routers, user access to the network (which includes log in credentials and networked shared folders and devices) is controlled by the campus AD or Active Directory. Network credentials are setup to expire every 30 days which requires campus users to change their passwords; this helps to prevent unauthorized access to a user's computer should that unit become infected with a virus or malware. Access to shared folders is strictly limited to the respective departments and only department heads can authorize access to their department's shared folder by someone outside of their department. All employees are required to adhere to the campus information security policy they are required to read and sign.

Lastly, all servers and workstations are monitored 24/7 by the campus anti-virus suite known as Symantec EndPoint; the software is designed to actively monitor the network and to block any potentially hazardous traffic and files that are suspicious or considered dangerous by the threat database provided by Symantec which is updated every evening. In the event an employee suspects their unit may have become compromised, they are to follow the procedure described in the information security policy. In addition to the anti-virus, Nunez utilizes a program known as Spybot Search and Destroy which is designed specifically to prevent Malware from entering a work station; because of its ever changing base code, Malware at times can bypass a virus scan as its code base is of a different characteristic and therefore can be missed.

Communications:

As a standard practice, Nunez faculty and staff are not to divulge Personal Identifiable Information (PII) to 3rd party vendors or partners in the clear, meaning that no electronic communications containing the PII of a student or employee will be transmitted via email or unsecured link; files containing such information will be transmitted to the appropriate party via a security server by the authorized personnel only.

Database Access:

Nunez faculty and staff have access to two databases containing PII: The Banner system and the FX legacy system. Banner access rights are granted only after the appropriate forms have been filled out electronically and authorized by the campus authorizer for each section; no access will be granted by the Banner campus security administrator without the approval of the appropriate section head.

Access to the FX legacy system has been reduced from a network resource to the database being contained on stand -alone units not connected to the infrastructure; these units are designated for archival purposes which will allow staff to go back and check a student records that may have not been converted to Banner. With these computers not being connected to the infrastructure or internet, unauthorized access is prevented.

Breach Notification:

In the event a database breach is detected, Nunez Community College will inform the affected parties by certified letter and a follow up phone call to ensure the party has been properly informed. Nunez will assist the affected party in signing up with a free credit monitoring service to further safe guard against additional identify theft.

X	Reviewing Council/Entity	Review Date	Effective Date
X	Office of Information Technology	10-2018	11-9-2018
X	College Compliance Committee	11-2018	11-9-2018
X	Chancellor's Council	11-9-2018	11-9-2018

Policy Referenced: Louisiana Database Breach Notification Law SB205 Act 409.

Distribution: Distributed Electronically via College's Internet 1-14-2019

Chancellor's Signature/Approval

SIGNATURE:_____ DATE: 11-15-2018

Tina M. Tinney, Ed.D.
Chancellor