Nichols College
Security Incident Response Policy

1.0 Policy Statement

The Nichols College Information Technology (IT) Security Incident Response Policy and procedures define standard methods for identifying, tracking and responding to network and computer-based IT security incidents.

2.0 Scope

This policy covers the College's general response, documentation and reporting of incidents affecting computerized and electronic communication information resources, such as theft, intrusion, misuse of data, other activities contrary to the College's Acceptable Use Policy, denial of service, corruption of software, computer and electronic communication-based privacy violations (including MASS Law 93H, regulation CMR 17.00, HIPAA, etc.) and incidents reported to Nichols College by other institutions and business entities. This policy does not include damage to personal computers owned by students, unless their computers contribute to the incident defined by the parameters in Definitions below.

3.0 Purpose

The Nichols College IT Security Incident Response Policy is established to protect the integrity, availability and confidentiality of confidential or proprietary information, including PII (Personally Identifiable Information) to prevent loss of service and to comply with legal requirements. This policy establishes the coordination of the College's response to computerized and electronic communication systems incidents to enable quicker remediation, information gathering and reporting of infrastructure affected and security related events.

4.0 Definitions

An **IT Security Incident** ("Incident") is any activity that harms or represents a serious threat to the whole or part of Nichols College's computer, telephone, or network-based resources such that there is an absence of service, inhibition of functioning systems, including unauthorized changes to hardware, firmware, software or data, unauthorized exposure, change or deletion of PII, or a crime or natural disaster that destroys access to or control of these resources. Routine detection and remediation of a "virus", "malware" or similar issue that has little impact on the day-to-day business of the college is not considered an Incident under this policy.

5.0 Policy

5.1 Identification of Incidents

Any member of the Nichols College community or individual or organization outside of Nichols College may refer an activity or concern to IT. The IT department can also identify an Incident through its proactive monitoring of the College's network and information system activities. Once identified, IT will use standard internal procedures to log and track Incidents and, working with others as appropriate, take steps to investigate, escalate, remediate, refer to others or otherwise address as outlined in the remainder of this policy.

5.2 Establishment of an IT Security Incident Response Team

The IT department is responsible for Incident interdiction and remediation of computer and electronic communication based resources affected by these incidents. The IT department will consult key representatives of IT, administrators in affected departments, Public Safety, Communications, legal, or other units, as warranted to establish an IT Security Incident Response Team appropriate to respond to a specific Incident.

5.3 Documentation and Communication of Incidents

The IT department will ensure that Incidents are appropriately logged and archived. Any IT Security Incidents involving PII will be so identified in order to implement the relevant procedures. The CIO will provide incident reporting to the Vice President for Administration. The VP for Administration will make the determination on whether it is reasonable and appropriate to invoke the Nichols College Emergency Response Team, given the circumstances of the Incident.

Wherever possible, documentation of such Incidents will cross-reference other event databases within the college, such as the IT Help Desk request system, network monitoring systems, and Public Safety reporting system.

The CIO will be responsible for communicating the Incident to appropriate personnel and maintaining contact, for the purpose of update and instruction, for the duration of the Incident.

5.4 Protocols and Procedures

The IT department will maintain standard protocols and procedures for the response and investigation of each Incident, as well as securing the custody of any evidence obtained in the investigation. The procedures will specify the location and method of custody for each incident, if custody of evidence is required.

5.5 Role of Nichols College Personnel, Training

All employees are required to report Incidents, or suspected Incidents, to the IT Help Desk (x2206, helpdesk@nichols.edu).

5.6 Incident Prevention

Wherever possible, the college will undertake to prevent Incidents by monitoring and scanning its own network and systems for anomalies, and developing clear protection procedures for the configuration of its IT resources.

6.0 Special Situations/Exceptions

Any personally-owned devices, such as smart phones, tablets, laptops, wireless devices or other electronic transmitters which have been used to store PII and are determined to contribute to an Incident, may be subject to seizure and retention by Nichols College Public Safety until the Incident has been remediated, unless the custody of these devices is required as evidence for a court case. By using these devices within the Nichols College network for business purposes, individuals are subject to College policies restricting their use.

7.0 Effective date

This Security Incident Response Policy is effective January 1, 2015. The College will review this Policy on a regular basis and reserves the right to change, modify, or otherwise alter this Policy at its sole discretion and at any time as it deems circumstances warrant.