# Policy Title: Information Technology Security Incident Response

**Impact:** Employees, Students, Affiliates

**Responsibility:** Chief Information Officer

**Effective Date:** 3/28/2018

**Revised Date:**

**Reviewed Date:**

**Relates to Procedure(s):** 3.08.04

**Legal Citation(s):**

## I. Information Technology Security Incident Response

All North Idaho College (NIC) users of Information Technology (IT) resources must report "IT Security Incidents" to the IT Helpdesk, chief information officer, or an IT director as soon as they are aware of such activity.

IT security incidents will be handled based on the type and severity of the incident. An Incident Response Management Team will oversee the handling of all IT security incidents involving restricted data.

All individuals involved in investigating a computer security incident will maintain confidentiality.

A. Definitions

1. "Affiliate" refers to any authorized individual, business, or organization connected to NIC, authorized to act on behalf of NIC, or authorized to conduct work related to NIC needs.

2. "Information Technology" or "IT" refers to any resource related to the access and use of digitized information, including but not limited to hardware, software, devices, appliances, network bandwidth, and resources.

3. An Information Technology (IT) Security Incident ("Incident") refers to theft, loss, misuse, exposure, or other activity that harms or threatens the whole or part of NIC's computers, information systems, data, telephone, and network-based resources.