

# Asheville-Buncombe Technical Community College

# (A-B Tech) Procedure

## Procedure #1007: Reporting Suspicious IT Activity

The Vice President of Operations/Chief Information Officer (CIO) is charged with the oversight of this policy and procedure, and for supervising implementation of these procedures, consistent with College policy.

Step 1

If an employee encounters suspicious activity, as defined in the policy, that employee shall *not* attempt to mitigate said activity.

Step 2

The employee shall contact the IT Helpdesk without delay to report the matter. The employee is encouraged, but not required, to forward any evidence, such as the suspicious email in question.

Step 3

Information Technology will investigate the matter upon receiving notification that an employee has reported suspicious activity. In so doing, IT reserves the right to limit or restrict access to College technology. Additionally, IT reserves the right to inspect, copy, remove, or otherwise alter any data, file, or system resource that might have been undermined.

Step 4

If the situation warrants, the College may require the employee to maintain a level of confidentiality surrounding the matter. If the suspicious activity is indicative of an attack, Information Technology will document the incident and the response, and such documentation shall be made public upon request.

As this procedure is consistent with Policy 1007: Reporting Suspicious IT Activity, no employee will be personally penalized or rebuked for reporting suspicious activity.

References: See Policy 1007: Reporting Suspicious IT Activity

Owner: Vice President of Operations/CIO

Updated: August 12, 2019