

Information Security Policies

Network Monitoring

Version 1.0

Effective Date:

9-23-11

Approved by:

IT Advisory

Committee

Network Monitoring Policy

1.0 Purpose

The purpose of this policy is to outline Keuka College policy regarding the monitoring, logging, analysis and retention of network packets that travel on the Keuka College physical network.

2.0 Scope

Individuals affected:

This policy applies to all students, faculty, and staff attending or employed by Keuka College who access, handle, use or otherwise connect to the college's information technology resources (also referred to as *users*). In addition, the designation user also refers to all visitors, subcontractors, potential students, research associates, media representatives, and non-college entities or individuals who are granted access to Keuka College's information technology resources.

Resources covered:

This policy applies to all college resources, whether individually controlled, shared, stand alone or networked. It applies to all computers and communications devices owned, leased, operated or provided by Keuka College. This includes, but is not limited to personal computers, wireless communication devices, networking devices, workstations, servers, and any peripheral devices and the associated software thereof. This policy also applies to all privately owned devices used to store, process or transmit college owned data.

3.0 Policy

Monitoring traffic at Keuka College will be limited to packet header information, not the packet data itself unless required to check for viruses, to monitor for improper release of confidential data, or for intruder detection.

Two departments are authorized to monitor data traffic; Information Technology Services and <Keuka's security office>.

Intranet traffic may be monitored at the request of individual departments at the discretion of the Dean, Department Head, or Director. If network traffic is monitored for reasons other than routine network operations, diagnostics or maintenance the individual department will justify the network monitoring to the Director of Information Technology Services before monitoring takes place.

Faculty, Staff and Students should be aware that logs are generated during the course of accessing network services. Though it is not the practice of Keuka College to actively

monitor Internet traffic, it is sometimes necessary to monitor such traffic in order to diagnose network problems.

4.0 Enforcement

Information Technology Services will use information about traffic flow to enforce provisions set forth in the Antivirus Policy and Network Acceptable Use Policy, The Network Monitoring Policy, Keuka College Information Resources Policy, other College Policies and State and Federal Laws.

Compliance:

At minimum these principles must be followed by individuals while connected to Keuka College resources. Individual departments may apply stricter standards, provided they do not conflict with the standards and procedure outlined in this document.

5.0 Definitions

Users – Faculty, Staff, Students, and other members of the Keuka college community that use or interact with the Keuka College network in any fashion.

Packet Header Information – The Packet Header refers to supplemental data placed at the beginning of a block of data being stored or transmitted.

6.0 Revision History

6/12/2011 – Document Created

7.0 Policy Impact Statement

The ability to monitor network traffic will substantially aid in the enforcement of the acceptable use and other policies concerning network traffic. In addition network monitoring provides valuable data about network requirements and capabilities.