| | |
|---|---|
| NAME: | **Monitoring and Investigation of Files/Network Connection Policy** |
| ISSUING DEPARTMENT | Campus Technologies |
| ISSUED DATE: | 1998 |
| REVIEWED DATE: | |
| APPROVING AUTHORITY: | |
| DATE REVISED: | February 2015 |

DEFINITION

Just because we have the ability to view information, it does not mean we should. Monitoring of another person's electronic activity or network connections without their prior consent (for instance: assistance from a helpdesk technician) shall not be entered into lightly.

PURPOSE

It is the intention of this policy to outline the procedure for monitoring and investigation

SCOPE

This procedure concerns all Mansfield University Personnel.

FORMS

N/A

RESPONSIBILITY

Campus Technologies

PROCEDURE

The following procedures outline when and how monitoring of a person's electronic activity shall be performed.

1. A request to consider monitoring a person's electronic activity without their prior consent must come from a supervisory authority and as an allegation of a violation of the technology Appropriate Use Policy. Reference: http://ct.mansfield.edu/policies-procedures/
2. The request to consider monitoring shall be directed only to the President, Provost or the Chief Information Officer. Utmost care will be exercised to preserve the integrity of the campus communication systems for the intended academic and administrative purpose by authorized users of that resource.
3. The person receiving the request to monitor activity shall communicate with the other two individuals so that the President, Provost, and the Chief Information Officer are all aware of the situation.
4. All employees of the Commonwealth of Pennsylvania are obligated as part of their normal work environment to the strictest confidence in the access and disclosure of sensitive or confidential information where it exists on a computer

or network in any of its forms. IF employees of Campus Technologies, in the course of their work, observe activity that may be harmful to campus systems and/or network (such as programs being launched to attack servers, users attempting to break into accounts, unauthorized servers, etc.), the technology personnel shall take precaution to remove the problem pc or software from the network and report this activity to the Chief Information Officer. The CIO will take any further actions as necessary to protect the integrity of the campus communications systems affected and notify the President and the Provost of the action.

5. The results of any monitoring or activity discovered shall be kept in the strictest of confidence by Campus Technologies personnel assigned and communicated only to the Chief Information Officer who shall promptly forward the results to the President and the Provost.
6. In the case of monitory activity of a faculty or staff member, the President in consultation with the Provost shall decide what action, if any, shall be taken as a result of the monitoring. In the case of monitoring the activity of students, the Chief Information Officer in consultation with the Provost and the Vice President of Student Affairs shall decide what action, if any, shall be taken as a result of the monitoring. Campus Police will be notified if investigation warrants their participation and campus policies for investigations and disciplinary actions will apply.

DISTRIBUTION

This policy will be distributed through the web and maintained by Campus Technologies.