

Academic Computing & Networking Investigation of and Response to Policy Violations

Note

The issues addressed in this document deal with procedures associated with violations of Academic Computing & Networking (AC&N) policies. AC&N's role in investigating or addressing violations of other campus policies such as academic dishonesty is not addressed in this document.

Background

As the operational administrator of the campus network and central academic computing resources, Academic Computing & Networking (AC&N) has an obligation to protect the resources it manages for the campus. To satisfy this obligation, AC&N monitors and addresses policy violations as they relate to these resources. Policy violations may come to our attention via an external or internal complaint, may be discovered in the normal course of business, or may be brought to our attention in some other way.

When a policy violation occurs or is alleged, the action taken will depend on the specific violation and the circumstances associated with it. The following types of questions and issues may be considered, along with other relevant facts or circumstances, in determining how AC&N staff will proceed with respect to investigating and resolving the violation or alleged violation:

- Is the alleged activity interfering with normal operations of shared resources such as the campus network or central computer systems or servers?
- Are campus resources at risk of being damaged or compromised?
- Is the alleged activity impacting access or performance for other users?
- Has this activity occurred before?
- Does the alleged activity suggest a violation of federal, state, or local law has occurred?
- Do the circumstances require or suggest that a law enforcement agency be contacted?
- Have we received a proper notice of alleged copyright infringement compliant with Digital Millennium Copyright Act requirements?
- Does the alleged activity violate other campus policies or the student honor code?
- Have we received proper legal notification, court order, subpoena or warrant seeking activity information, data or file content?
- Have we received a directive from an appropriate CSM administrative authority to take some action or conduct an investigation?

Actions

AC&N is responsible for ensuring that the resources managed by AC&N are accessible, operational, and fully functional. Although AC&N staff are authorized and may be compelled to temporarily suspend accounts and disable network connections when a policy violation is discovered or computing resources are compromised, AC&N does not administer disciplinary action. When AC&N becomes aware of a policy violation that is not being addressed by law enforcement authorities or through another campus office or process, AC&N staff may recommend an appropriate response and sanctions or disciplinary action to the Vice President in whose area the offending party is employed or enrolled. Specific actions taken when the violation is discovered and/or after the investigation is completed will depend upon the nature of the violation and the circumstances associated with it.

In all cases, AC&N staff will

- take whatever immediate action is deemed appropriate to protect the security and operation of the campus network, computer systems, computer accounts, and other resources managed by the department if those resources appear to be misused or compromised,
- comply with federal, state, and local law, and campus policies,
- cooperate with law enforcement and government agencies as required by law.

Process

In general, when a policy violation is alleged or discovered, we will do the following:

1. Determine if the alleged or observed violation is creating problems for, causing harm to, or has the potential to cause harm to campus resources. If, in our judgment, campus resources are negatively impacted, then whatever action is required to stop immediate harm, prevent further damage, and protect campus resources will be taken without notice. This may include temporary suspension of accounts, disconnecting systems from the campus network, termination of running programs and processes, shutting down or otherwise disabling resources, or any other action deemed necessary.
2. Determine if we are required by law to report the alleged or discovered activity to law enforcement. Whatever action is required to comply with law will be taken without notice.
3. Provide information to University counsel as directed by appropriate CSM administrative authorities to comply with court orders, warrants, subpoenas, or state or federal law such as the DMCA or USA Patriot Act. In some situations, we may have to provide information without notifying you first, and may be required by law to provide the information and not inform you at all.
4. Investigate or address complaints or discoveries of alleged violations of AC&N and CSM computing and networking policies as follows:
 - a. Some complaints that we receive may involve your alleged use of CSM's network or other resources in a manner that violates a license agreement or infringes upon the rights of a copyright holder. In these cases, we are notified as the administrator of the network to which your computer was or is attached.
 - i. If, in our judgment, the complaint is from a known and credible source, we may forward a copy of the complaint to you directly with a request that you take action. You may also receive instructions from us as to what you must do to prevent services provided by CSM from being suspended.
 - ii. If, in our judgment, the complaint is from an unknown or suspect source, we will investigate further and may refer it to University Counsel and/or contact you if appropriate.
 - iii. Depending on the nature and extent of the activity and whether it is a repeat offense, we may seek institutional disciplinary action, including termination of computing and networking services, by filing a complaint with the appropriate CSM administrative authority.
 - b. We will examine the circumstances and facts to determine what, if any, action we take next. System activity and transaction logs, performance data, and other transaction records may be examined as part of the investigation. Content of email and other files will not be examined as part of a routine investigation, except in the following circumstances:
 - i. Files of any type whose protection is set to be "world readable" may be examined.
 - ii. A court order or other legal method requires that we examine and disclose content.
 - iii. We are instructed in writing by appropriate CSM administrative authorities to examine content and provide information to University Counsel as part of an internal campus investigation.
 - iv. We are conducting an internal AC&N investigation relating to system or network performance problems or behavior that indicates that specific user files need to be examined to identify a cause. In this situation, two staff members must agree that the examination is necessary and the director of AC&N must approve it.
 - c. Most policy violations will be addressed through routine procedures involving education, warnings, or temporary service suspensions (with or without notice depending on circumstances). However,
 - i. If we discover activity that suggests that another CSM department or law enforcement should be involved, we will make those contacts or referrals.
 - ii. If we receive a complaint about an issue that should be addressed by a different department, we will refer the complainant to the appropriate department.
 - iii. If our investigation concludes that your activity warrants further investigation, institutional disciplinary action, or referral to appropriate law enforcement authorities, we will recommend such action to the appropriate CSM administrative authority and may refer the case to University Counsel or law enforcement authorities, if appropriate.
 - iv. If our investigation finds that your activity is a repeat offense and merits further action, we may tailor our sanctions accordingly and/or seek institutional disciplinary action such as termination of services by filing a complaint with the appropriate CSM administrative authority.

Examples of how this process may be applied in specific types of situations are summarized below. Incidents may be handled differently from these examples based on the specific circumstances.

Examples

- 1. If your account appears to be in use by someone other than you, or if your password is determined to be "crackable" by an automated program that we run:**
 - a. Your account may be temporarily suspended without warning. We cannot send an e-mail to you about this since that would pose a security risk for your account and CSM systems.
 - b. You must contact us in person with proof of identity (a valid student or staff ID) to get your account reactivated.
 - c. If we have evidence that you are deliberately sharing your account with others, we may file a complaint with the appropriate administrative authority requesting disciplinary action.
- 2. If you are consuming (in the opinion of the resource manager) unreasonably large amounts of a shared resource (such as disk space, processor time, or network bandwidth):**
 - a. Access to that resource (including your network connection) may be temporarily suspended to improve service for all users while we investigate the cause.
 - b. If the excessive resource consumption appears to be accidental, we may attempt to contact you to resolve the situation. If service is suspended without warning, however, you should contact us to determine why your service was suspended. We will discuss the issue with you and work with you to resolve the situation if appropriate.
 - c. In all cases, we will take immediate steps to protect resources and the ability of other users to use those resources.
 - d. If our investigation concludes the excessive use appears to be purposeful, malicious, designed to cause service problems for others, ignores your responsibility to others to fairly share resources, or is caused by activity that violates our policies or involves criminal or illegal activity, we may present evidence to the appropriate administrative authority and recommend disciplinary or legal action. In such cases, service will be restored while the complaint is pending only at the request of the administrative authority considering the complaint.
- 3. If we receive a properly filed notification or complaint alleging copyright, trademark, or licensing infringement:**
 - a. You will receive a copy of the complaint via e-mail with instructions as to what you must do to restore services that may have already been suspended, or to prevent further action such as suspension of network services.
 - b. If you comply with the instructions, no further action will be taken by AC&N unless this is a repeat complaint or there are aggravating circumstances.
 - c. If you do not comply with the instructions, further action will be initiated and may include, but is not limited to:
 - i. Suspending network and/or other computing services
 - ii. AC&N staff referring the matter to the appropriate administrative authority (such as the Dean of Students, Dean of Graduate Studies, or a Vice President) for disciplinary action
 - d. If we are instructed by University Counsel and/or receive a court order, or subpoena, or request pursuant to and compliant with the terms of the Digital Millennium Copyright Act (DMCA) to provide log, contact, or other information, then if we have such information, we will provide it.
- 4. If we receive a complaint from on- or off-campus about your activities or use of resources we manage:**
 - a. We will first evaluate the nature of the complaint and determine if it needs to be referred to another party such as law enforcement authorities or another office within the institution.
 - b. If we do not refer the complaint elsewhere, we will investigate the situation and, if appropriate, notify you that a complaint has been received and ask you to respond to us.
 - c. If our investigation of the complaint causes us to discover violations of our policies, we will require you to cease the activity that is causing the violation and instruct you as to what you must do to prevent further action by AC&N. If you fail to respond or refuse to comply, we may seek disciplinary action through the appropriate administrative authority. If we determine that services for other users are being negatively

- impacted because of your activities, your services may be temporarily suspended while the matter is reviewed by the appropriate administrative authority.
- d. If our investigation of the complaint does not reveal any violation of our policies, we may refer the original complainant to the appropriate law enforcement agency or CSM office or department, if they wish to pursue their complaint further.

5. If we discover a violation of policy during our routine course of business:

- a. If, in our judgment, the violation is negatively impacting services for other users or is creating a security risk for you or our resources, your services may be temporarily suspended without warning. If you find that your service has been suspended, you should contact AC&N support staff as soon as possible to determine the reason. If appropriate, we will work with you to resolve the situation.
- b. We will notify you that the activities causing the violation must cease and advise you if we intend to refer the matter to the appropriate authority. If appropriate, we will also instruct you as to what you must do to avoid further action by AC&N.
 - i. If you fail to respond or refuse to comply, we may refer the matter to the appropriate administrative authority for disciplinary action.
 - ii. If we determine that services for other users are being negatively impacted because of your activities, your services may be temporarily suspended and we may refer the matter to the appropriate administrative authority for disciplinary action. In this case, service will be restored while the complaint is pending only at the request of the administrative authority considering the complaint.