AC&N Incident Reporting

The Colorado School of Mines takes all complaints about inappropriate traffic originating from our network seriously and encourages anyone who suspects a problem to contact us. The CSM Office of Computer Security is responsible for coordinating the response to complaints regarding violations of AC&N computer and network usage policies.

Examples of Complaints to Report to AC&N:

- Email-viruses from computers attached to the CSM network. If you do receive a virus please verify that it came from CSM, as many viruses spoof the sender so that the email appears to originate from a trusted source. Viewing the full headers should help you determine the IP address of the originating system.
- Hacking or cracking of any kind.
- Unwanted email (SPAM) that has originated from a CSM computer. Unfortunately we can not help with email that originated outside the CSM network. Please see the AC&N Spam Management web page (http://www.mines.edu/email/spam/) for help dealing with unwanted email.

Examples of Things to Report to Other CSM Offices are:

- If you are having any experience that you feel is harassing or threatening, please contact the appropriate authority immediately. If you are not sure who to report the activity to, please contact CSM Public Safety. ***If you feel that you are in immediate danger, call 911.***
- Copyright holders wishing to file a complaint under the Digital Millennium Copyright Act (DMCA) should see our DMCA policies page (http://www.mines.edu/all_about/policy/dmca.shtml) or contact the CSM AC&N DMCA team directly.

Reporting an Incident to AC&N:

To help us respond to your report appropriately we need as much information as possible. At a minimum we will need the following information:

- The time of the incident being reported including time zone.
- The IP address or hostname of the computer that received the suspect traffic.
- The email address that received suspect traffic.
- The IP address or hostname that was the source of the unwanted traffic/email.

In addition, any of the following will facilitate our response:

- If you are reporting a hacking attempt, we need to know the type of traffic (ICMP, TCP or UDP) and any port numbers or service names you may have.
- If the traffic was detected by a firewall or an intrusion detection system, any relevant log entries.

- If you are reporting an email virus or SPAM, please include the original message with all headers, as an attachment to your report.
- Any additional information you may have is always welcome.

When reporting an incident please use the following contact guidelines:

- If you are being actively attacked or are experiencing a loss of service, please call the AC&N main number at (303) 273-3431 and ask to be transferred to someone in the network or security office.
- If you are not currently experiencing problems, please send your report via email.
- For more information about contacting us, including copies of public keys that will be used to sign all communication, please see our contacts page.

What to expect:

You should expect to receive an emailed acknowledgment of your complaint within 24 business hours. We may also ask for additional information to help us investigate your report.

If the attack is currently in progress, you should expect the traffic to stop shortly after we have verified your report. If the traffic does not stop, please call the main AC&N number, (303) 273-3431, and ask to be transferred to someone in the network or security office.

Once we have completed the investigation of a complaint, we will email a summary of our findings. Due to legal restrictions on the release of information about our students, this summary is typically very brief. Under normal circumstances we will acknowledge that we have found the source of the traffic and have dealt with any issues. We will, of course, also report anything we find that suggests a serious security threat to your systems.

HISTORY AND REVIEW CYCLE

The policy will be reviewed at least annually, or as needed by the Responsible Administrative Unit.