****

**Purpose**

The purpose of this procedure is to define the process followed when a network abuse notice is received, to define the classification levels of network abuse notices and to establish a process for documenting and mitigating network abuse notices.

**Background**

Effective July 1 2010, the U.S. Department of Education enacted the Higher Education Opportunity Act (HEOA) Peer to Peer provision that requires all colleges and universities to comply with three general requirements regarding unauthorized file sharing on campus networks:

* An annual disclosure to students describing copyright law and campus policies related to violating copyright law
* A plan to effectively combat the unauthorized distribution of copyrighted materials by users of its network, including the use of one or more technology-based deterrents
* A plan to offer alternatives to illegal downloading

**Network Abuse Notification Procedure**

1. **Network Abuse Notification**

Network abuse notifications are initiated by and received from the Board of Regents Information Technology Services (ITS) and other external entities such as the Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA) when evidence of infringement has been detected from a system on the campus network.

 Network abuse notices are classified as follows:

* *Urgent* – Business interruption issue that could halt production (e.g., imminent security threat)
* *High* – A malicious activity having a potentially negative impact on networks, systems, and data (e.g., denial of service attack, unauthorized access)
* *Low* – An activity that exploits vulnerabilities in applications, protocols and services that does not directly result in a service compromise (e.g., spam, virus, probe)

Roles and Responsibilities

* BOR ITS – logs network abuse notices from entities in the USGTrack-It system
* BOR ITS – sends network abuse notices to abuse@savannahstate.edu
* Systems Security Manager – receives, monitors and responds to abuse notices
* CSIT Network team – locates identified host and applies controls to the network
* CSIT Helpdesk – remediates identified host
1. **Network Abuse Controls, Host Discovery and Resolution**

Upon receiving a network abuse notice, the host discovery and resolution process is initiated.

**Network Abuse Controls**

Technology-based deterrents are used to effectively combat unauthorized peer to peer file sharing on the campus network. A packetshaper is used to manage bandwidth utilization through policy-based rules that limit the ability of peer to peer functions. By default, the firewall allows only incoming traffic that has been explicitly permitted to prevent hosts from acting as servers.

**Host Discovery Process**

1. The network abuse notice is examined by the Systems Security Manager to collect information about the affected host, the abuse notice classification, and infringing activity.
	1. A determination is made as to whether the host is on the wired or wireless network and a communication is sent to the appropriate administrator to locate the host.
2. The Network team traces wired hosts to a switch port on the campus network.
	1. Orion is used to detect hosts on the campus network.
3. The Systems Security Manager traces wireless hosts on the residential network (ResNet).
	1. Network Admission Control (NAC) is used to detect hosts on the ResNet.
4. For campus hosts, a HelpDesk ticket is created to remediate the affected host.

**Host Resolution Process**

A tiered approach is defined for employees and students based on the network abuse notice classification, offense level and network type.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Abuse Classification** | **Offense Level** | **Network Type** |
| **Employee** | **Urgent/High** | **1st Offense** | **Wired/Wireless** |
|  | 1. Disable the network switch or wireless NAC port.
2. Open a HelpDesk ticket for system remediation with information regarding the host (IP/MAC address, switch port, infringement, date).
3. For wired connections, the user will be contacted for instructions on the corrective action for the violation.
4. For wireless connections, the user is re-directed to a NAC restricted-access web page informing them of the violation and corrective action.
5. Corrective Action:
6. Review the P2P File Sharing Policy.
7. Complete the IT Security for End-users training.
8. Re-enable network port.
 |
| **Employee** | **Low** | **1st Offense** | **Wired/Wireless** |
|  | 1. Send a “Network Abuse Warning” letter to the user.
 |
| **Employee** | **Urgent/High** | **Repeat Offender** | **Wired/Wireless** |
|  | 1. Disable the network switch or wireless NAC port.
2. Open a HelpDesk ticket for system remediation with information regarding the host (IP/MAC address, switch port, infringement, date).
3. For wired connections, the user will be contacted for instructions on the corrective action for the violation.
4. For wireless connections, the user is re-directed to a NAC restricted-access web page informing them of the violation and corrective action.
5. Inform the user, user’s supervisor and HR of the violation.
6. Corrective Action:
7. Submit a signed statement to the Systems Security Manager that validates the user has read and understands the P2P File Sharing Policy.
8. Complete the IT Security for End-users training.
9. Re-enable network port.
 |
| **Employee** | **Low** | **Repeat Offender** | **Wired/Wireless** |
|  | 1. Send a “Network Abuse Warning” letter to the user and the user’s supervisor.
 |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Abuse Classification** | **Offense Level** | **Network Type** |
| **Student** | **Urgent/High** | **1st Offense** | **Wired/Wireless** |
|  | 1. Disable the network host.
2. Open a HelpDesk ticket for system remediation with information regarding the host (IP/MAC address, switch port, infringement, date and other pertinent information).
3. For wired connections, the user must contact the HelpDesk for instructions on the corrective action for the violation.
4. For wireless connections, the user is re-directed to a NAC restricted-access web page informing them of the violation and corrective action.
5. Inform Student Affairs (VP) of the violation.
6. Corrective Action:
7. Review the P2P File Sharing Policy.
8. Complete the IT Security for End-users training.
9. Re-enable network port.
 |
| **Student** | **Low** | **1st Offense** | **Wired/Wireless** |
|  | 1. Send a “Network Abuse Warning” letter to the user and Student Affairs (VP).
 |
| **Student** | **Urgent/High** | **Repeat Offender** | **Wired/Wireless** |
|  | 1. Disable the network host for the semester.
2. Open a HelpDesk ticket for system remediation with information regarding the host (IP/MAC address, switch port, infringement, date and other pertinent information).
3. For wired connections, the user must contact the HelpDesk for instructions on the corrective action for the violation.
4. For wireless connections, the user is re-directed to a NAC restricted-access web page informing them of the violation and corrective action.
5. Inform Student Affairs (VP) of the violation.
6. Corrective Action:
7. Submit a signed statement to the Systems Security Manager that validates the user has read and understands the P2P File Sharing Policy.
8. Complete the IT Security for End-users training.
9. Re-enable network port at the beginning of the new semester.
 |
| **Student** | **Low** | **Repeat Offender** | **Wired/Wireless** |
|  | 1. Send a “Network Abuse Warning” letter to the user and Student Affairs (VP).
 |

1. **Network Abuse Reporting**

After remediation of the network abuse, the Systems Security Manager responds to the originating source of the network abuse notice with the resolution.

**Other Information**

|  |  |
| --- | --- |
| Community Awareness: | SSU Peer to Peer Policy |
| Legal Alternatives: | <http://www.educause.edu/legalcontent> |
| FAQs: | <http://www.respectcopyrights.org/faqs.html> |
| Federal Copyright Law Penalties: | <http://www.educause.edu/Resources/Browse/HEOA/34600#annual> |