

## **Operational Procedure Suspension or Permanent Termination of IU Information Technologies (IT) Access**

### **Introduction**

If a user puts the IU network at risk by consistently engaging in activities which cause security compromises of the network or engage in activities which are either explicitly illegal or in violation of IU policy, IT's only recourse is to disable the user's network access. Network access refers to lab/CTS use, connectivity from user-owned equipment, connection via wireless or in student housing and/or the user's IU Network ID account. This document defines the appropriate process for suspension or permanent termination of network access.

The "appropriate disciplinary office" for students is Judicial Affairs; for staff, it is a department head and Human Resources; for faculty, a department chair or Dean.

### **Suspension of IT Access**

ITPO policy IT02 states:

**"Suspension or termination of access:** Service managers, system administrators, and security and network engineers may temporarily suspend or block access to an account when it reasonably appears necessary to do so in order to protect the integrity, security, and functionality of university or other computing resources, or to protect the university from liability.

... Before removing access for staff or faculty who are also students, the department should consult with the appropriate campus Dean of Students or equivalent."

Suspension of IT access may occur without notice to the user where there is reason to believe that the user is committing unlawful acts with IU computing resources, the user's actions may constitute a liability on the part of the University or where there is reason to suspect there is an immediate danger to the network.

Offenses are categorized as being either "malicious" or "culpable" (see below). This process specifically affects lab, classroom technology, VPN, wireless or housing access when a user has engaged in either malicious activity or when the number of culpable offenses become excessive. Malicious offenses may result in immediate IT access termination or suspension depending on the severity of the offense.

Level One: The IT Information Security Officer (ISO) will provide an email notification to the user explaining the type of activity in which the user engaged as well as a citation of the resultant violation(s) and ask the user to stop engaging in that activity. This email requires a response from the user within 24 hours. If the user does not respond in 24 hours, IT will disable access for that user, (lab/CTS access if the violations occur in labs or classrooms, or MAC address blocking if related to wireless or housing). The access is to remain blocked until such time that the user acknowledges that (s)he understands IU IT policy and has ceased the activity related to the notice. IT will provide a pointer to any relevant IU policies as well as a notification that another violation will result in a suspension of the user's IT access for a period of 15 days.

Level Two: If the user continues to engage in inappropriate activity (in conjunction with the appropriate disciplinary office), the IT ISO will email the user referencing the previous warning(s), a statement of the recourses available to IT, a pointer to all relevant IU policies, notification that his/her access will be suspended for 15 days, an indication that another violation will result in a suspension of their access indefinitely and that the potential exists for the permanent revocation of IT privileges. IT will suspend relevant access for 15 days. The appropriate disciplinary office and the VCIT will be CC-d on the email. Again, if the user does not respond within 24 hours, the appropriate access avenue will be blocked.

Level Three: If, after the first two incidents, a user engages in inappropriate activity, the IT ISO will email the user (in conjunction with the appropriate disciplinary office) copies of previous warnings and notice that the lab, CTS, wireless and/or housing access, (depending on the avenue(s) of the infraction) is to be permanently terminated. The email will be CC-d to the appropriate disciplinary office and the VCIT. A request will then be placed with IU South Bend IT for the user's access to be suspended, (MAC address blocking and disable network port in housing). The user will be notified that further violations may result in the suspension or termination of their IU IT account.

Final Recourse: **Suspension/Termination of IT Network ID Account.** In the event the user continues to utilize his/her IU IT account to engage in inappropriate activity, the IT ISO will make a request to the appropriate disciplinary office to suspend or terminate the user's IU Network ID account. A letter will be sent to the user's last known address indicating the action being taken (CC-d to the appropriate disciplinary office and the VCIT). A request will then be placed with UITS for the user's IU Network ID account access to be suspended/terminated.

Suspension Reinstatement: Before a user may have their IU Network ID account reinstated following a formal suspension, the user will be required to sign the "Reinstatement of IU Computing Privileges User Agreement." All parties will be made aware that one more incident will result in the permanent termination of the user's IU Network ID account with no opportunity for reinstatement.

## **CATEGORIES AND TYPES OF POLICY VIOLATIONS**

### **Malicious**

- Illegal activities including but not limited to copyright infringement.
- Accessing or attempting to gain unauthorized access to another computer resource (i.e., port scans, unauthorized use of a computer, hacking attempts, etc.).
- Unauthorized service on the network (examples: breaches of IT-19, connecting a server to the network, operating an unauthorized FTP server/proxy server/DHCP server/router, setting up an unauthorized wireless access point or bridge, etc.).
- The unauthorized use of someone else's IT account.
- Use of IU resources to harass other people.
- Any attempt to circumvent network security.
- Unauthorized data access.
- Knowingly engaging in activity which creates an unnecessary risk or liability to the University.
- Continued engagement in any activity that a University official has specifically warned the user against.
- Using IU resources to operate an unauthorized business.

### **Culpable**

- Being infected with viruses that pose a threat to the IU network by either providing unauthorized access to the infected computer, being part of a BOT net, being used to attempt to infect other computers, being used to send out spam email or otherwise impede other users or excessively affecting the IU network.
- Sharing IT access in a method in opposition to IU policy.
- Excessive use of network resources.