Misuse and Abuse of Information Technology Resources

IT-02

About This Policy

Effective Dates:
05-23-2006

Last Updated:
08-17-2011

Responsible University Administrator:
Office of the Vice President for Information Technology & Chief Information Officer

Policy Contact:
University Information Policy Office, uipo@iu.edu

Scope

This policy applies to all users of Indiana University information technology resources regardless of affiliation, and irrespective of whether those resources are accessed from on-campus or off-campus locations.

Policy Statement

Indiana University will handle misuse and abuse of information technology resources in accordance with existing policies and procedures issued by appropriate authorities. The university may also take legal action against individuals or entities involved in misuse or abuse of university information technology resources.

Reason For Policy

Taxpayers, students, and other groups providing sources of funding that support information technology resources at Indiana University expect that these assets will be used in a lawful manner and in support of the university's mission of research and creative activity, teaching and learning, and civic engagement.

Procedure

Reporting:
Reports of apparent misuse or abuse of Indiana University information technology resources are to be made to the following offices or authorities:

1. For the Bloomington and IUPUI campuses, contact the University Information Policy Office (UIPO) at it-incident@iu.edu.
2. For all other campuses, contact the regional campus Chief Information Officer (CIO) and the regional campus Chancellor's Office (for allegations involving academic appointees), the regional campus Human Resources Office (for allegations involving staff), or the regional campus Vice Chancellor for Student Affairs (for allegations involving students).
3. Where violations of law are alleged, contact the UIPO (for Bloomington/IUPUI) or the regional campus CIO, as well as, campus police and/or University Counsel.

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.

Access to university technology resources may be removed immediately given a written request from the appropriate university authorities, the supervisor or executive administrator of an employee, or the sponsor of

the account. Reasons for removal may include, but are not limited to, the following: the individual is terminated for cause and there is concern for safety of systems or data; there is reasonable belief that the individual to whom the account is assigned has perpetrated or is involved in illegal activities or activities that violate university policy. Before removing access for staff or faculty who are also students, the department should consult with the appropriate campus Dean of Students or equivalent.

The technician responsible for a particular service may disable access unilaterally if processes in an assigned account are causing or reasonably appear likely to cause damage to systems or data or serious service degradation for other users. Except when prohibited by law, inappropriate, or impractical, the technician will notify the involved individual prior to disabling the computer account. Where prior notification is not permitted, appropriate, or practical, the technician will make all efforts to notify the involved individual afterward in a timely manner. Unless other policies are invoked, access will be restored as soon as possible after the removal of the threat.

Technical Investigation: The University Information Policy Office (UIPO) will coordinate technical investigation and computer forensics for complaints of misuse or abuse of university information technology resources. For campuses other than Bloomington and IUPUI, the regional campus Chief Information Officer (CIO) will consult with UIPO in conducting the necessary investigation and data gathering. All investigations will comply with applicable law, and university policies and procedures. Disciplinary Process: Reports of misuse or abuse are normally resolved through established university disciplinary policies and procedures applicable to the relevant user. The university may also refer suspected violations of applicable law on the part of any individual to appropriate law enforcement agencies. Indiana University Police, University Counsel, and other law enforcement officials as appropriate shall address misuse or abuse of Indiana University resources by persons not affiliated with the university. Consultation: The University Information Policy Office (UIPO) and/or regional Chief Information Officers (CIOs) are available to provide consultation or advice related to technology use or misuse to any university, campus, or unit administrators or individual personnel.

Definitions

Information technology resources
includes all university-owned computers, peripherals, and related equipment and software; voice communications infrastructure, peripherals, and related equipment and software; data communications infrastructure, peripherals, and related equipment and software; all other associated tools, instruments, and facilities; and the services that make use of any of these technology resources. The components may be individually controlled (i.e., assigned to an employee) or shared single-user or multi-user; they may be stand-alone or networked; and they may be stationary or mobile.

Misuse or abuse
are uses of Indiana University information technology resources that violate existing laws or university policies and procedures (including but not limited to University Information Technology Policies; the Code of Student Rights, Responsibilities, and Conduct; the Academic Handbook; University Human Resources Policies; and University Financial Policies), or that otherwise violate generally accepted ethical norms and principles. Misuse or abuse also includes the sharing or transferring of an individual's university accounts, including network ID, password, or other access codes that allow them to gain access to university information technology resources, with one or more other persons.

Regional campus Chief Information Officer:
The primary responsibility of a regional campus Chief Information Officer is the development and use of information technology in support of the campus's vision for excellence in research, teaching, outreach, and lifelong learning. He or she is also responsible for disseminating information to the campus, coordinating activities that involve more than one campus, fostering cooperation in areas such as sharing technical expertise and training, and problem coordination and resolution for their own campus information technology issues.

University Chief Information Officer:
The primary responsibility of the University Chief Information Officer is the development and use of information technology in support of the university's vision for excellence in research, teaching, outreach, and lifelong learning.

The University Information Policy Office (UIPO) represents the University Chief Information Officer (CIO) with respect to policy issues related to the IU Bloomington and IUPUI campuses.

Sanctions

Indiana University will handle reports of misuse and abuse of information and information technology resources in accordance with existing policies and procedures issued by appropriate authorities. Depending on the individual and circumstances involved this could include the offices of Human Resources, Vice Provost or Vice Chancellor of Faculties (or campus equivalent), Dean of Students (or campus equivalent), Office of the General Counsel, and/or appropriate law enforcement agencies.

Failure to comply with Indiana University information technology policies may result in sanctions relating to the individual's use of information technology resources (such as suspension or termination of access, or removal of online material); the individual's employment (up to and including immediate termination of employment in accordance with applicable university policy); the individual's studies within the university (such as student discipline in accordance with applicable university policy); civil or criminal liability; or any combination of these.

History

- Reviewed December 2011.
- Revised August 17, 2011: changed titles in *Sanctions* section to more accurately reflect current usage.
- Revised March 4, 2010: enhancing language in *Sanctions* section
- Approved May 23, 2006
- Posted as an interim policy September 5, 2000