

If the publication is to be printed off campus, the Director of University Publications, through the requesting department, submits all printing specifications and a list of acceptable vendors via a purchase requisition to the Purchasing and Central Receiving Department which conducts a bidding process. The printer is selected on the basis of pricing, quality, and ability to meet the specifications. An Indiana State University purchase order or use of an authorized University procurement card is required in advance of any obligation of funds governed by the University.

In addition to coordinating the bidding process with the Purchasing and Central Receiving Department, the University Publications Office acts as a liaison between the initiating office and the printer. University Publications will submit the purchase requisition as part of the bidding process and will bill the initiating office.

University Directory

The University Directory lists names, home addresses, office numbers, and home and campus telephone numbers of faculty and staff. The directory is compiled from information provided by individuals. All faculty and staff members are asked to complete a directory information sheet prior to the beginning of the fall semester. The sheets are provided by the University Publications Office. The directory also contains a student listing compiled from student registration information.

Publications Permissions Policy

As a protection to the University and its contributors, Indiana State University copyrights each issue of certain of its publications. Any writer who wishes to use material from these publications should contact the appropriate editor or the University Publications Office.

CAMPUS SERVICES

Mail Service

ISU provides mail delivery and pick up at designated times and locations. Campus mail should be addressed to an individual or a department rather than a building and/or room number. Use of campus mail is intended for University business only. Personal mail should be directed to the home address.

Mail intended to be sent through the U.S. Postal Service will not be metered without a departmental budget account. If a mailing piece reaches the mail room without postage or a budget account, it will be returned to the issuing department. As a courtesy to faculty and staff, stamped personal mail is collected from specified locations.

Unauthorized use of campus mail by non-related University organizations (profit or non-profit) as well as local business advertising and solicitations is prohibited by the U.S. Postal

Service. Mailing pieces which proselytize religious or political groups may not be sent via campus mail.

The University Campus Mail Service is located in the Facilities Management building at 951 Sycamore Street. For questions regarding hours of operation, pick up and delivery times, postal rates and other pertinent information, the mail service may be contacted at 237-8043.

INFORMATION TECHNOLOGY RESOURCES

The University is committed to an open flow of information within and between the University and the public. Those who use University information resources are to take reasonable and necessary measures to safeguard the operating integrity of the systems and their accessibility by others while acting to maintain a working environment conducive to carrying out the University's mission of instruction, research and scholarship, and public service.

Information resources at the University, including access to local, national and international networks, are available to support students, faculty and staff. The Office of Information Technology, under the direction of the Provost and Vice President for Academic Affairs and with University community advice, provides development and management of the centrally supported digital infrastructure and related services, and proposes policies related to information technology resources.

The following policies introduce issues of legitimate use, information security, and privacy that arise in the use of computers, software, and electronic information. These policies strive to balance the individual's ability to benefit fully from these resources and the University's responsibility to maintain the accessibility, integrity, utility, and security of the electronic information environment.

University Responsibilities

The University owns or leases most of the computers and computer networks used on campus and has various rights to the software and information residing on, developed on, or licensed for these computers and networks. The University has the responsibility to administer, protect, and maintain its aggregation of computers, software, and networks.

Specifically, the responsibilities of the University are to:

1. Ensure efficient and reliable performance of University computer systems and networks.
2. Establish and support reasonable standards of security for electronic information that University community members produce, use, or distribute.
3. Protect University computers, networks and information from destruction, tampering, unauthorized inspection and use.

4. Ensure that information technology resources are used in a manner consistent with the University's mission.
 5. Delineate the limits of privacy that can be expected in the use of networked computer resources and preserve freedom of expression over this medium without countenancing unlawful activities.
 6. Ensure that University computer systems do not lose important information because of hardware, software, administrative failures or breakdowns. To achieve this objective, authorized systems or technical managers may occasionally need to examine the contents of system files to diagnose or solve problems.
 7. Communicate University policies and individuals' responsibilities systematically and regularly in a variety of formats to all parts of the University community.
 8. Monitor policies and propose changes in policy as events or technology warrant.
 9. Manage computing resources so that members of the University community benefit equitably from their use.
 10. Enforce policies by restricting access in case of serious violations (see section on "Sanctions").
4. Identify oneself accurately and appropriately in electronic communications.
 5. Use resources efficiently. Accept limitations or restrictions on computing resources such as storage space, time limits, or amount of resources consumed when asked to do so by authorized personnel. University resources are to be used in a manner consistent with the University's mission. Indiana State University computing resources may not be used for commercial purposes.
 6. Recognize the limitations to privacy afforded by electronic services. Users have a right to expect that what they create, store, and send will be seen only by those to whom permission is given. Users must know, however, that the security of electronic files on shared systems and networks is not inviolable – most people respect the security and privacy protocols, but a determined, technically-well-informed person may be able to breach them. Users must also note that, as part of their responsibilities, systems or technical managers may occasionally need to diagnose or solve problems by examining the contents of system files.
 7. In addition, an individual's right to privacy may be superseded by the University's responsibility to maintain the network's integrity. Should the security of the network or a computer system be threatened, a person's files may be examined by an OIT administrator with approval from the Provost and Vice President for Academic Affairs or Associate Vice President for OIT or designee. Finally, by law, instances can arise when material created or received via electronic means must be divulged (i.e., pursuant to a validly issued subpoena in connection with legal action).

Individual Responsibilities

Indiana State University supports networked information resources to further its mission and to foster a community of shared inquiry. All members of the University community must be cognizant of the rules and conventions that make these resources secure and efficient. It is the responsibility of each member of the University community to:

1. Respect the right of others to be free from harassment or intimidation to the same extent that this right is recognized in the use of other communications media. Consequently, although each user has the right to freedom of speech, unlawful material may not be sent or displayed to others.
2. Respect copyright and other intellectual property rights. Unauthorized copying of files or passwords belonging to others or to the University may constitute plagiarism or theft. Modifying files without authorization (including altering information, introducing viruses or Trojan horses, or damaging files) is unethical and may be illegal.
3. Maintain secure passwords. Users should establish appropriate passwords in the first instance, change them occasionally, and not share them with others. This is necessary to maintain privacy and to assure accountability as a consumer of University resources.
8. Learn to use software and information files correctly. Users should maintain and archive backup copies of important work. Users are responsible for backing up their own files. If users depend upon OIT backup service, they should become familiar with the schedules and procedures of that service.
9. Abide by security restrictions on all systems and information to which access is permitted. Users should not attempt to evade, disable, or "crack" passwords or other security provisions; these activities threaten the work of others and are grounds for immediate suspension or termination of privileges and possible further sanctions.
10. Abide by all applicable federal and state laws. Indiana State University extends these principles and guidelines to systems outside the University that are accessed via the University's facilities (i.e., electronic mail or remote logins using the University's Internet connections). Network or computing providers outside Indiana State University may also impose their own conditions of appropriate use for which users at this University are responsible. For

violations of the above, see the "Sanctions" section of this policy.

Sanctions

Individuals or groups who act in a manner contrary to existing policy and accepted standards for computer use or who take actions which have legal implications are subject to appropriate sanctions. Indiana State University reserves the right, at all times, to suspend or revoke the privilege of access to University electronic services. Violations of information technology policies will be dealt with in the same manner as violations of other University policies and may result in disciplinary review.

As a first step, such matters will be addressed by the appropriate Office of Information Technology (OIT) administrator. Whenever it becomes necessary to enforce University rules or policies, the University may take the following steps, and any other steps it deems appropriate to address the use or misuse of University electronic services.

An authorized OIT administrator may:

1. Disallow network connections by certain computers (departmental or personal).
2. Require adequate identification of computers and users on the network.
3. Undertake audits of software or information on shared systems where there is sufficient reason to suspect policy violations.
4. Take steps to secure compromised computers that are connected to the network.
5. Restrict or deny access to computers, the network, and institutional software and databases.
6. Refer the matter for disciplinary action.

Users are expected to cooperate with authorized investigations either of technical problems or of possible unauthorized or irresponsible use as defined in these guidelines; failure to do so may be additional grounds for suspension or termination of resource access privileges.

If a matter is not resolved in discussion with the OIT administrator within 24 hours, the OIT administrator's action may be appealed to the administrator's direct supervisor or referred to the appropriate University administrator for resolution in a timely manner. Any revocation of privileges is subject to the normal due process available to all members of the faculty, staff and student body. In addition, certain kinds of abuse (such as copyright violation, fraud, violation of software licenses, or harassment) may entail initiation of civil or criminal

investigation and/or prosecution.

Additional questions relating to information technology resources policies should be directed to the Executive Director, Office of Information Technology.

Use of Computer Software

Indiana State University is committed to the appropriate use of software. With few exceptions, most software is copyrighted. Any software used on a University-owned computer must have a valid license. Software delivered through the network is properly licensed. If software is installed or upgraded on a University computer, it is the individual's responsibility to ensure licensing requirements have been met. Suspected violations of copyright and other applicable laws will be reported to appropriate University authorities.

Copyrighted Video Programs

Most programs from commercial or public television broadcasts are protected by copyright. Use of such programs in the University, whether for classes or for other purposes, could constitute violation of the copyright laws. The taping and public showing without explicit permission of programs carried on cable or pay television is a violation of the law. The taping and public showing of copyrighted dramatic works from broadcast television is also a violation. However, some allowances are made for showing in the educational setting. Such activity is termed "Fair Use" and is defined in copyright laws. In a non-profit university, non-dramatic literary or musical works recorded off the air may be shown in places normally devoted to instruction if the work is directly related to instruction. The institution may not profit financially from the showing.

It is the policy of the University to uphold the letter and spirit of the law in copyright and other issues. Members of the University community who violate the law do so at their own risk and without the support of the University. They will be subject to curtailment of their privileges within the institution and to civil or criminal prosecution from without.

File Sharing Programs University Owned Computers

The purpose of this policy applicable to all ISU computers, is to help ensure the stability, performance and security of ISU's networked environment, protect sensitive information on individual computers, and aid in compliance with federal and state copyright laws.

Definitions

File Sharing Programs - programs that function in a peer-to-peer

structure and are designed to share files (music, video, software, images, etc.). Examples of such software include, but are not limited to: AudioGalaxy, Gnutella, KaZaA, WebShots and Morpheus.

ISU Computers-all computers owned, and or operated, by or on behalf of Indiana State University (ISU).

Statement of Policy

File sharing programs will not be installed on Indiana State University computers (except as noted under "Exceptions").

The Office of Information Technology (OIT) will maintain a current list on its website of all applications covered by this policy. The list will be changed as new applications of this type are developed.

If file-sharing programs are observed on Indiana State University computers (other than those covered under "Exceptions" noted below), the head of the office or department concerned will take such actions as are necessary to have the program immediately removed. If necessary, appropriate disciplinary actions will be taken to ensure that no others will be installed.

If a faculty member claims an exemption under "Exceptions" noted below, and if such program causes problems for the network or such use results in allegations of violation of copyright, OIT will contact the employee to attempt to resolve the issue. If OIT cannot resolve it, the matter will be referred to the appropriate dean.

In all cases, when technical issues affecting other computers are not resolved in a timely fashion, OIT is authorized to disconnect the system from the network until such corrections can be accomplished. In such an event, a formal notice of action will be provided to the responsible parties and his/her direct superior.

Exceptions

Equipment used by faculty who have installed such programs on their assigned computers as part of their teaching and research efforts are exempted from this requirement. Faculty who elect to install the programs will take all necessary action to protect their computers, and the information that may be in the storage media, from the adverse effects of these programs. In the event a program is affecting other computers, it must be removed. Faculty must also ensure that any downloading or sharing of materials complies with copyright laws.

Security of Data

Federal and state laws with regard to privacy and security have become increasingly complex. A network of overlapping federal and state law places a fiduciary obligation on the University to protect the privacy, use, and security of select

data. Laws include, but are not limited to: Electronic Communications Privacy Act (ECPA), Computer Fraud and Abuse Act (CFAA), Family Education Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act (GLBA), etc. This policy is intended to define the limits of that obligation and the duties and responsibilities of University employees to safeguard information that constitutes protected data.

Data is considered to be a University resource and as such, policies controlling the collection, use, and dissemination of data are set by the University. ISU employees are expected to know the policies pertaining to data and to abide by their provisions. Access to data by ISU personnel is granted on a need to know basis consistent with their job function.

Definitions

Data - Numerical or other information represented in a form suitable for processing by computer; factual information, especially information organized for analysis or used to reason or make decisions. For purposes of this policy, data is intended to be defined broadly and is understood to mean all information collected by Indiana State University in the conduct of its business as an educational institution, and any information stored on Indiana State University servers/workstations, or distributed using the ISU network.

Data Classifications - the following definitions shall be used to classify data at ISU.

- Public open access data - data that is not personal in nature that requires minimal protection. Threats to data are minimal, and only minimal precautions to protect the data need to be taken. Alteration or destruction of the data is the primary concern.
- Public limited access data - data that has limits on access either by contractual arrangements or by the nature of the data. Access is usually restricted to ISU staff and student use. Unauthorized access, alteration, or destruction of the data is the primary concern.
- Private releasable data - data that is personal in nature but that has been designated as public information (examples are first and last name). Some data in this category can be designated as private by the individual (example is unlisted phone number). Such designation must be in writing – data so designated will be considered "private sensitive data". Alteration or destruction of the data is the primary concern.
- Private non-sensitive data - data whose disclosure would not involve issues of personal credibility, reputation, or other issues of personal privacy and where release of the data is not an overriding concern (example is change of major). Unauthorized access,

alteration, or destruction of the data is the primary concern.

- Private sensitive data - data whose disclosure involves issues of personal credibility, reputation, or other issues of personal privacy protected by law (examples are Social Security number, birthday, and student grades). Data in this classification is often mandated by law but can be so designated by the trustee office responsible for the data. Unauthorized access, alteration, or destruction of the data is the primary concern.
- Restricted/Critical data - data of a sensitive nature that requires a high degree of protection (example is credit card information). Unauthorized access, alteration, or destruction of the data is the primary concern.

Handling of Data

- Public open access data - data can be stored and disseminated using minimal protection. Data can be transported using non-secure methods. Data can be transferred to other non-University owned machines and can be widely distributed.
- Public limited access data - data can be stored and disseminated using minimal protection. Data can be transported using non-secure methods. Data can be transferred to other non-University owned machines but can't be shared outside of ISU.
- Private releasable data - data can be stored and disseminated using minimal protection. Data can be transported using non-secure methods and can be shared outside of ISU on a business need basis.
- Private non-sensitive data - data can be stored and disseminated using minimal protection. Access is limited on a need to know basis. Data can be transported using non-secure methods. Unless specified to the contrary, data defaults to this category. Data can be transported using non-secure methods and can be shared outside of ISU on a business need basis.
- Private sensitive data - data is limited on a need to know basis. Data must be kept on centrally supported servers and may be stored in encrypted form. Data may be stored on workstations as needed for short periods of time necessary for processing but must be encrypted and protected from unauthorized access. Access to data is controlled centrally by a user ID and password. All data being distributed over the network must be encrypted. Hardcopy containing data must be shredded when no longer needed for the intended purpose.

- Restricted/Critical data - data is highly controlled and accessible on a strict need to know basis. Data storage is restricted to servers only and no data will be moved to a workstation for storage. Data must be stored encrypted on central servers that provide both network security (i.e. behind firewall) as well as physical security. Workstations that have access to the data must be located in a physically secured area (locked room/limited access); all write-able media devices removed (i.e. diskette drives, etc.); no software except that required to perform the designated work function is permitted and the workstation must not be connected to the Internet. Data must be encrypted at all times and hardcopy containing restricted/critical data must be shredded when no longer being used.

Control of Data Access

- Username (ID) and passwords – access to controlled data shall be accomplished through the use of usernames (ID) and passwords. (please see “Use of Passwords” policy for further details.)
- Access to controlled data (like IDs and passwords) are not to be shared with other employees. As noted above, data dissemination is driven by 1) the classification of the data, and 2) the need to know.
- Student IDs that access ISU data other than public data will be supervised by full-time ISU personnel; the use of the student ID shall be the responsibility of the full-time employee.
- Classification and access to controlled data shall be the responsibility of the office designated as the trustee for the respective data (for example, Human Resources would be the trustee for employee data). Disagreements on data classification and access will be resolved by the Chief Information Officer (CIO).
- Data requiring encryption will be protected by a generally recognized encryption scheme (examples are PGP, Excel encryption, etc.) – use includes digital signatures for email and encryption of stored data.
- Employment policies and procedures relating to compliance with data security policies will be developed by Human Resources.

There are no exceptions to this Security of Data Policy.

Computer Network/Server Security

Indiana State University provides network services to a large number and variety of users – faculty, staff, students, and external constituencies. Security compromises for any campus-networked system can have a detrimental impact to

other systems housed on the University network infrastructure. The Office of Information Technology (OIT), in cooperation with University constituents, has campus-wide responsibility to maintain the integrity and security of networking systems and to provide the wiring, cable and wireless network infrastructure supporting voice, data and video services.

This policy is necessary to ensure the stability, performance and security of the Indiana State University network environment. Data is an institutional asset. Therefore, it is appropriate and applies to establish policies to ensure the protection, integrity, and reliability of data. This policy encompasses all systems directly connected to OIT-maintained networks or systems on networks that receive network service from Indiana State University network resources. The policy includes, but is not limited to, campus local area network connections, modem pools and DSL connections. OIT is required to provide reasonable protection consistent with federal and state laws placing fiduciary obligation on ISU to protect the privacy, use and security of select data. Laws include, but are not limited to: Electronic Communications Privacy Act (ECPA), Computer Fraud and Abuse Act (CFAA), Gramm-Leach-Bliley Act (GLBA), the United States Patriot Act (USPA), Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act of 1996 (HIPAA) and others. This policy is intended to define the limits of that obligation and the duties and responsibilities of University employees to safeguard information that constitutes protected data to all ISU computer network resources.

Definitions

- A. Indiana State University Computers and Networked Resources – all computers and network resources (e.g. routers, switches, firewalls, print servers, remote access servers) owned or operated by or on behalf of Indiana State University.
- B. Network Traffic – defined broadly is the flow of data within the confines of the Indiana State University network, and traffic flowing from the ISU network through the Internet service provider.
- C. Network Server – defined broadly is a computer physically connected to the ISU data network for the purpose of sharing or distributing its resources such as printers, files, and programs. This definition is not intended to include desktop workstations that are supporting peer-to-peer file or printer sharing.
- D. Network Servers Residing in High Risk Area – consists of those servers that sit between the Internet and the ISU network's line of defense which are commonly some combination of firewalls or similar network security appliance.
- E. Host Based Intrusion Detection Systems – systems that

use an automated tool or set of tools designed to detect security violations by analyzing the data source and to respond with appropriate actions.

- F. Wireless Network Access – unlicensed spread spectrum radiofrequency wireless local area network access. This access permits connectivity to the ISU network.
- G. Remote Access – the ability to get access to a computer or a network from a remote location. This may occur via telephone lines or a secondary internet service provider.
- H. Network Management – the execution of the set of functions required for controlling, planning, allocating, deploying, coordinating, and monitoring the resources of a data network.
- I. Physical Network Security – controlled access to areas which house network infrastructure components such as data electronics and physical cable plant.

Statement of Policy

OIT will monitor all network traffic (intra-campus, inbound and outbound Internet, DSL service, and modem connections) to ensure proper network management and performance. The Chief Information Officer or her/his designee will determine, with the advice of the Information Technology Advisory Council (ITAC), criteria for proposed changes to traffic limitations and recommend those that are consistent with the academic and business goals of the University.

OIT will maintain a registry of all servers resident on the ISU network in order to ensure proper accountability and communications between all parties responsible for server support and operation.

Servers used and managed by academic departments for instructional and/or research purposes are permitted. Registration of such servers is required and can be accomplished using the online form located at the OIT website. Such registration is intended for the identification of the resource on the network to facilitate communications and is not intended to imply control over the functional use of the server.

All other servers (those that support administrative, business, or office functions or process, servers that house institutional data subject to federal, state or local law, or servers that act as the primary repository for institutional data shall be administered and managed by OIT.

If servers are placed on the University network without proper registration, OIT staff will attempt to contact the appropriate individual(s). If contact cannot be made, OIT personnel are authorized to disconnect the server from the University network until such time as proper registration is completed.

Servers shall conform to guidelines set forth in the server High

Risk Area document located at the OIT website—Server configuration parameters are published on the OIT website. This is the University Office of Information Technology recommended configuration document library. This library contains general and operating system-specific guidelines.

OIT will assist academic departments in determining the proper level of security to implement on servers residing in high-risk areas. Systems behind the firewall must be secured. This will minimize the potential for damage by intruders. Academic departments establishing servers will consult with OIT to determine appropriate security solutions for their environment. OIT will provide one or more valid IP addresses for dedicated systems, depending on demonstrated need. OIT will configure and maintain all network firewall devices. Information concerning changes to individual unit firewall services configuration and routine maintenance actions will be communicated to departmental contact person(s).

Network filtering devices will not be set up as a firewall without approval from OIT. While these type firewall systems can provide excellent functionality, there are a number of potential problems with using them. These problems include, but are not limited to: 1) the security of the host system itself must be maintained; 2) Operating System firewall systems are often difficult to configure and maintain, requiring significant system administration skills and may result in excessive coordination responsibilities for OIT staff; and 3) an improperly configured operating system firewall may cause problems for other systems on campus. If problems exist with a network filtering device, OIT personnel will attempt to contact the appropriate individual(s). If contact cannot be made, OIT personnel are authorized to disconnect the system from the University network until such time that a technical resolution is found.

Host based intrusion detection systems will be installed on all mission critical desktop systems. OIT shall provide an initial configuration that will be used by University personnel during first time installation. Deviations from the initial configuration for an individual or a department host based intrusion detection system shall be documented by OIT personnel. A list of currently supported host based intrusion detection systems may be obtained by contacting the OIT help desk.

To ensure the technical coordination required to provide the best possible wireless network for Indiana State University, OIT will be solely responsible for the management of 802.XX and related wireless standards access points and wireless access security on the campus. Departments may deploy 802.XX or related wireless standards access points after appropriate coordination with OIT. When deploying any wireless access point, departments must register the access point device with OIT. Departments are strongly encouraged to utilize OIT services for all activities related to wireless network access. These activities include pre-engineering/consultation, site survey, installation, and management. A registration form is available at the OIT website and further wireless network access guidelines may be

found there. OIT will perform network scans for unregistered wireless access points. If an unregistered wireless access point is identified, OIT personnel will attempt to contact the appropriate individual(s). If contact cannot be made, OIT personnel are authorized to disconnect it from the University network until such time as the access point is properly registered. Any department wireless access point that interferes with another system will be disconnected until the problem is resolved.

OIT provides remote access services to the University community and while OIT encourages departments to use this service, remote access does present a security issue. When a department identifies the need for remote access, it must register the remote access device(s) with OIT. A registration form is available at the OIT website. Remote access system guidelines are contained in the OIT recommended configuration document library found at the OIT website. If remote access servers or systems are placed on the University network without proper registration, OIT personnel will attempt to contact the appropriate individual(s). If contact cannot be made, OIT personnel are authorized to disconnect these from the University network until such time as proper registration is completed.

As the central support entity for the Indiana State University data network, OIT is assigned the following responsibilities and authority:

- OIT, or its designee, is authorized to perform a security audit of any ISU network device(s) at any time.
- OIT is the primary contact for all network security related activities.
- OIT will prepare network recommendations and guidelines and will post them on OIT web pages. OIT will publish security alerts, post vulnerability notices and patches, and disseminate other pertinent information to assist in preventing security breaches.
- OIT will coordinate investigations into any alleged computer or network security compromises, incidents, and/or problems. Suspected security problems and issues may be reported to OIT via e-mail to itcert@isugw.indstate.edu, or by calling extension 2910.
- OIT will monitor backbone network traffic in real-time as necessary and appropriate to detect unauthorized activity or intrusion attempts. All monitoring will be carried out in compliance with the policies contained in the Indiana State University Handbook.
- If network scans or monitoring identify security vulnerabilities that could jeopardize the University or the ISU network, the cooperation of the system owners and system managers will be solicited to accomplish necessary corrective action. If the appropriate contact cannot be

made, the head of the system owner's/system manager's department will be notified. When a server experiences a problem that constitutes a serious security issue or negatively impacts the ISU network on a global basis, OIT will take steps to disable network access to that system and/or device until the problem(s) has/have been rectified.

To ensure physical network security, access to network distribution centers is limited to those individuals whose work requires access to rooms that house network electronics and physical cable plant.

There are no exceptions to this policy.

Use Of Passwords

Security for University-owned data systems and the information they contain is a primary concern. While a variety of means are used to achieve system and data security, the use of a username and password remain one of the most effective means of providing security for, and protecting access to, data. Stated in another way, passwords are the "keys" to a system.

In order to ensure that proper use of password protection is implemented, it is necessary for the University to define a set of minimum standards for the use of passwords.

Definitions

Password – a protected/private string of alphanumeric characters used to authenticate an identity or to authorize access to data. A password is a group of characters used in conjunction with a username (or user ID) to achieve security by permitting access to data, information, or facilities that would be otherwise inaccessible.

Username – the name or user ID assigned to each individual that identifies that individual to various systems and network resources.

Statement of Policy

Passwords should follow the generally accepted technology industry standard. Specifically a good password has the following qualities:

- Has at least eight characters — The shorter the password, the generally easier it is to crack.
- Is made up of characters, numbers, and symbols — Numbers and symbols hidden within letters (or vice versa) lengthens the possible number of options for a given password, which strengthens the overall password.
- Is unique — Select passwords that are different than other passwords you may be using. If all of your

passwords are the same or very similar, the magnitude of a security breach can be much greater.

- Are not dictionary words — By using dictionary words as passwords, you are making it exponentially easier for your system to be cracked. Don't do it, and don't override authentication schemes that prevent the use of dictionary words to allow your users to do it.
- Are not tied to your personal information — If you use passwords that are your birthday, spouse's name, or the make of your car, you are asking for trouble. Think about every password you use and determine whether or not someone who knows you could guess it. If there is even a slight chance they could, don't use that password.
- Can be typed quickly — If your password is so complicated that you must hunt-and-peck for the characters each time you type it, prying eyes could easily watch your fingers and guess your password. At the very least, practice typing your password while alone to increase the speed in which you can type it.
- OIT shall have responsibility for all system level passwords. The passwords will be maintained in a central production database and shall be changed quarterly, at a minimum (passwords for IDs that have the capability to set security related items). IDs with system-level privileges must have different passwords from all other accounts owned by systems or network personnel that use the system-level accounts.

Users will be responsible for the protection of their individual password(s). User level passwords must be changed each six months at a minimum.

Passwords inserted in email, other electronic communication, or placed in a digital storage format must be encrypted. Passwords are not to be shared with anyone else.

Users should use different passwords for ISU accounts versus those used for non-ISU accounts.

There are no exceptions to this policy.

Use Of Electronic Mail

The University provides electronic mail resources to support its work of teaching, scholarly research, and public service. This administrative policy statement sets forth the University's policy with regard to use of, access to, and disclosure of electronic mail to assist in ensuring that the University's resources serve those purposes. This policy applies to all

faculty, staff and students who use the Indiana State University network and systems.

Statement of Policy

A. Privacy, Confidentiality and Public Records Considerations

Indiana State University will make reasonable efforts to maintain the integrity and effective operation of its electronic mail systems, but users are advised that these systems should in no way be regarded as a secure medium for the communication of sensitive or confidential information. Because of the nature and technology of electronic communication, ISU can assure neither the privacy of an individual user's use of the University's electronic mail resources nor the confidentiality of particular messages that may be created, transmitted, received, or stored on these.

In addition, Indiana law provides that communications of University personnel that are sent by electronic mail may constitute "correspondence" and, therefore, may be considered public records subject to public inspection under the Access to Public Records Act (IC 5-14-3-3).

B. Permissible Use of Electronic Mail

1. Authorized Users - Only ISU faculty, staff, and students and other persons who have received permission from the appropriate University authority are authorized users of the University's electronic mail systems and resources.
2. Purpose of Use - The use of any University resources for electronic mail must be related to University business, including academic pursuit. Incidental and occasional personal use of electronic mail may occur when such use does not generate a direct cost for the University. Any such incidental and occasional use of University electronic mail resources for personal purposes is subject to the provisions of this policy.

C. Prohibited Use of Electronic Mail

1. Prohibited Purposes
 - a. Personal use that creates a direct cost for the University is prohibited.
 - b. The University's electronic mail resources shall not be used for personal gain or for commercial purposes that are not directly related to University business.

D. Other Prohibited Uses - Other prohibited uses of electronic mail include, but are not limited to

- a. Sending copies of documents in violation of copyright laws.
- b. Inclusion of the work of others in electronic mail communications in violation of copyright laws.
- c. Capture and "opening" of electronic mail except as required in order for authorized employees to diagnose and correct delivery problems.
- d. Use of electronic mail to harass or intimidate others or to interfere with the ability of others to conduct University business.
- e. Use of electronic mail systems for any purpose restricted or prohibited by laws or regulations.
- f. "Spoofing": constructing an electronic mail communication so it appears to be from someone else.
- g. "Spam": mass sending of unsolicited electronic mail.
- h. Attempting unauthorized access to electronic mail or attempting to breach any security measures on any electronic mail system, or attempting to intercept any electronic mail transmissions without proper authorization.

E. University Access and Disclosure

1. General Provisions

- a. To the extent permitted by law, the University reserves the right to access and disclose the contents of faculty, staff, student, and other users electronic mail without the consent of the user. The University will do so when it believes it has a legitimate business need including, but not limited to, those listed in paragraph 3.D.3 (below), and only after explicit authorization is obtained from the appropriate University authority.
- b. Faculty, staff, and other non-student users are advised that the University's electronic mail systems should be treated like a shared filing system, with the expectation that communications sent or received on University business or with the use of University resources may be made available for review by any authorized University official for purposes related to University business.
- c. Electronic mail of students may constitute "education records" subject to the provisions of the Family Educational Rights and Privacy Act of 1974 (FERPA).

The University may access, inspect, and disclose such records under conditions that are set forth in the statute.

- d. Any user of the University's electronic mail resources who makes use of an encryption device to restrict or inhibit access to his or her electronic mail must provide access to such encrypted communications when requested to do so under appropriate University authority.

2. Monitoring of Communications

The University will not monitor electronic mail as a routine matter but it may do so to the extent permitted by law as the University deems necessary for purposes of maintaining the integrity and effective operation of the University's electronic mail systems.

3. Inspection and Disclosure of Communications

The University reserves the right to inspect and disclose the contents of electronic mail:

- in the course of an investigation triggered by indications of misconduct or misuse,
- as needed to protect health and safety,
- as needed to prevent interference with the academic mission, or
- as needed to locate substantive information required for University business that is not more readily available by some other means.

The University will inspect and disclose the contents of electronic mail when such action is not more readily available by some other means.

4. Limitations on Disclosure and Use of Information Obtained by Means of Access or Monitoring

The contents of electronic mail communications, properly obtained for University purposes, may be disclosed without permission of the user. The University will attempt to refrain from disclosure of particular communications if disclosure appears likely to create personal embarrassment, unless such disclosure is required to serve a business purpose or satisfy a legal obligation.

5. Special Procedures to Approve Access to, Disclosure of, or Use of Electronic Mail

Individuals needing to access the electronic mail communications of others, to use information gained from such access, and/or to disclose information from such access and who do not have the prior consent of the user

must obtain approval in advance of such activity from either the Chief Information Officer, the Provost or the President.

E. Disciplinary Action

Appropriate disciplinary action will be taken against individuals found to have engaged in prohibited use of the University's electronic mail resources.

F. Public Inspection, Retention, and Archiving of Electronic Mail

1. **Public Inspection of Electronic Mail:** Communications of University employees in the form of electronic mail may constitute "correspondence" and therefore may be a public record subject to public inspection under the Indiana Access to Public Records Act (IC 5-14-3-3).
2. **Retention and Archiving of Electronic Mail:** Electronic mail messages produced or stored using University resources will be subject to such retention and archiving requirements as may be established by appropriate University authorities.

There are no exceptions to this policy.

Email As Official Communications To Students

Email provides a convenient, timely, efficient, cost-effective, and environmentally-aware means of delivering information and communication to students. The University has a compelling business interest in establishing a policy that ensures that all students have access to an electronic form of communication and that such means are used as a standardized channel by faculty and other College staff as needed.

There is an increasing need for electronic communication with students. The University intends to establish email as an official communication mechanism with students. To that end, students, faculty, and staff must be provided with an appropriate formal notification (by way of policy adoption) that all formally designates email as an official means of communication with students.

Applicability

This policy applies to all students enrolled at Indiana State University.

Definitions

Email- The transmission of computer-based messages over

telecommunication technology. The term email is used synonymously with the terms such as e-mail and electronic mail.

Official University Email Address - The email account that is provided to each student free of charge and which resides on a University owned, specified, and operated email server with the Internet designation of 'indstate.edu' domain and that is provided for the purpose of supporting student mail.

Statement of Policy

Email is a valid mechanism for official communication with students at Indiana State University. The University has, and hereby exercises, the right to send official communications to students by email. The University has, and hereby exercises, the right to expect that students will receive email and will read email in a timely fashion.

All students will be assigned an official university email address. University communications may be sent to this official university email address with the expectation that such communication is formal and official and with no additional requirement to use other means communication to accomplish student notification. This official university email address will be maintained in the official university email directory for each student.

The University may, at its discretion, provide a mechanism that allows a student to have email forwarded from the official university email address to another email address of the student's choice. However, students who choose to have email forwarded to another email address do so at their own risk. The University is not responsible for email forwarded to any other email address. A student's failure to receive or read in a timely manner official university communications sent to the student's official email address does not absolve the student from knowing and complying with the content of the official communication.

This policy encompasses all official communication between the University and the student whether that communication is related to course-related academic, non-course related academic, or non-academic purposes. Faculty and staff may assume that a student's official university email is a valid mechanism for communicating with a student. Faculty may, at their choice, use email for communicating with students registered in their classes. Students receiving course related communications from their course instructors through the official university email will be responsible for compliance with course requirements.

There are no exceptions to this policy.

University-Related Websites Policy

Any website associated with Indiana State University, or using the designations "Indiana State University," "Indiana State," "ISU," "Sycamores," or other University-associated name, nickname, abbreviation, or symbol, whether established by an academic or administrative unit, a foundation or center, a group or individual, must adhere to the following:

- Ownership of the registered website name will be held by Indiana State University, and such registration will be made only by the Executive Director of Information Technology.
- Selection of the domain name for the registered website must protect the educational status of the official Indiana State University network.
- The primacy of the official Indiana State University website(s) and/or portal(s) must be secured and maintained.
- Appropriate hosting, server, bandwidth, and associated content and technical support must be secured and approved in advance.
- Website content must comply with all official University policies, standards, and practices included in the ISU Web Publications Policy, and in the current University Standards, policies on the use of the University seal, logo, and other ISU symbols, and other standards and practices, including those regularly posted on the official Indiana State University websites. The website may not be used to provide or deliver content to non-ISU sites that frame or otherwise juxtapose it with any other material in such a manner as to make it appear the content originated at the other location.

To assure compliance with the policy, the following procedures must be followed prior to the implementation of such websites:

1. Technical plan for the website, including name, technical requirements, support requirements, and security provisions, must be reviewed and approved by the Executive Director of Information Technology.
2. Content plan for the website, including name, use of University seal, logo, and other ISU symbols, general content, schedule for review and updating of the website content, and the ISU office to be responsible for compliance monitoring, must be reviewed and approved by the Office of Public Affairs.
3. Contract for the development and/or provision of the website must be reviewed and approved by the Purchasing and Central Receiving Department for conformance with existing University contracts and licensing for sale or licensing of University or

University-related products or services.

4. Use of University, symbols, logos and other trademarks on commercial websites (i.e., “.com” and other domain names that may be developed) must be approved by the Purchasing and Central Receiving Department.
5. Contract for the development and/or provision of the website must be reviewed and approved by University Counsel prior to appropriate formal ratification of the contract.

Additional procedures or documentation may be developed as appropriate in the implementation of this policy. Such documents will be posted on the Indiana State University Information Technology website, in the category “Computer Policies”.

The Executive Director, Office of Information Technology, or designee, will regularly review all websites with names related to Indiana State University for compliance with this policy and procedures. Any websites not in compliance will be notified and dealt with as provided in the ISU Web Publications Policy. Failure to comply with these policies and procedures may result in action including termination of the website and/or appropriate civil or criminal action against the website developers/providers/owners.

Definitions

Maintainer/Publisher/Information Provider: Person responsible for publishing and updating the information contained in World Wide Web pages.

Personal Page: A web page for an individual faculty member, staff member, or student.

Publication Page: The electronic equivalent of a printed publication.

Link: A one-way hypermedia connection from one site to another on the World Wide Web expressed as a “link to” or “link from” a web site or page of information.

System Files: Electronic files which include error and processing logs; system, application and user configuration files; and system and user administration files.

ISU Web Publications Policy

The University recognizes the value and potential of publishing on the Internet and so encourages and supports students, staff, and faculty to publish electronic information. Units and individuals may create World Wide Web pages (see “Definitions” section) that are consistent with the University’s mission.

The quality of information published by the University is an important element in maintaining the reputation and image of the University. This policy establishes the following minimum standards and procedures to assist the University community in ensuring that information published electronically follows the same high standards as other forms of University published information (print, audiovisual, etc.).

1. Contents of all electronic pages, including their associated links, on University equipment must follow University standards regarding nondiscrimination and should be consistent with the University’s mission.
2. All unit home pages and pages that are the electronic equivalent of a publication must contain the date of the last revisions, the name of the unit publishing the page and the email address or link for communicating to the unit information provider. Electronic publications are subject to all University policies and standards.
3. Copyright laws apply to electronic publishing as well as to print publishing. Information providers must have permission to publish the information, graphics, or photographs on their pages if they are not the author or creator.
4. University resources may not be used to create or display web pages primarily for personal business or personal gain, except as permitted by other University policies. Resources may not be used to provide or deliver content to non-ISU sites that frame or otherwise juxtapose it with any other material in such a manner as to make it appear the content originated at the other location.
5. The University home page will not link directly to personal pages. Faculty, staff, or student personal pages must follow the guidelines in this policy. The following statement must appear on all pages from which links occur to personal pages: “The views and opinions expressed in the following pages are strictly those of the page authors. The contents of these pages have not been approved by Indiana State University.”

Domain Naming

Indiana State University is the owner of certain Internet address (IP) space and has registered certain domain names for its use. The purpose of this policy is to preserve and control the Internet domain name resources of the University for support of its mission of teaching, research, and service.

Applicability

This policy applies to all students, faculty and staff who use the Indiana State University network and systems.

Statement of Policy

A. Indiana State University is the owner of the Internet address (IP) space 139.102.1.1 through 139.102.200.254 and 139.102.207.1 through 139.102.254.254, and uses the Internet domain name “indstate.edu”. ISU has also registered numerous other variants as a protection against the possibility of exploitation of University’s reputation by others. A list of these may be found at the OIT website.

ISU Internet (IP) addresses may not be registered for use with any other domain name except as permitted below.

B. Domain Name Service: The Office of Information Technology (OIT) is responsible for implementing Domain Name Service (DNS) for all systems connected to the campus network, and for coordinating this service with other campus units. DNS resolves names and network addresses for network routing to on-campus and off-campus destinations.

C. ISU Domain Names: ISU departments, programs and approved activities are eligible to use indstate.edu top level domain names upon request to Office of Information Technology. This request must be from a dean or department head and will either be approved by OIT staff or forwarded to the Chief Information Officer (CIO) for further consideration. Requests should be made to the Executive Director, Office of Information Technology.

Typically, a department or organization would apply for a domain name that implies its name, or function, as in the following examples.

<u>Unit</u>	<u>Domain</u>
a school:	nursing.indstate.edu
a program:	mba.indstate.edu
a service:	ftp.indstate.edu

To be considered for a top level name a server would need to be of global interest to the Indiana State University community (e.g. ithelp.indstate.edu).

D. Non-ISU Domain Names: Within the range of network addresses (IP) used by Indiana State University, all non-indstate.edu domains must be reviewed by the Web Advisory Committee (WAC), including aliases. To be considered, a non-indstate.edu name must be requested by a dean or department head, must be consistent with University policies, and it must be demonstrated why the requested name should not be within the indstate.edu domain. Requests should be sent to the Executive Director, Office of Information Technology. Use of the domain name must be recommended for approval by WAC before further consideration will be given by the CIO.

Non-ISU domain names may not be re-directed to an ISU

domain name without specific approval from the CIO. Requests for such approval will be handled as specified in the above paragraph.

E. Fees for Assignment of Domain Names: The department requesting a domain name other than indstate.edu is responsible for any costs associated with registering the domain name.

F. Naming Priority and Conflicts: Domain names generally reflect programs or activities. When there are conflicts in requested names, WAC will review and make recommendations based on relative priorities. In cases where a desired name or alias is already taken, OIT will explain the options. OIT will survey the database regularly to avoid naming conflicts and otherwise protect the interests of Indiana State University.

G. Unacceptable Domain Names: The Indiana State University network is for instruction and research use only, as indicated by the indstate.edu domain name suffix. In general, only domain names supporting this use, such as “.edu”, or “.org: or “.museum”, are hosted by ISU’s Domain Name Service. Suffixes such as “.com”, “.net”, etc., are not acceptable for ISU-hosted domain names. Inappropriate domain names – names that are not consistent with ISU’s mission and acceptable use policy – will not be approved.

Individuals and groups wishing to host servers, websites or networks that are outside the scope of the ISU acceptable use policy will be required to obtain Internet service and Domain Name Service from a local or national Internet Service Provider (ISP). If the request involves an ISU-owned IP address, the domain name must be cleared through the approval process outlined for indstate.edu host names.

H. Problem Resolution

In cases where faculty and staff are involved in creating or hosting an unacceptable domain name on a system that uses an ISU IP address, or re-directing a non-ISU domain name to an ISU domain name, OIT will first contact the individual and attempt to resolve the issue directly. If this fails, the head of the department concerned will be notified.

When undergraduate or graduate students are involved, whether in the residence halls network or elsewhere, OIT will contact the student first to attempt to resolve the issue. If OIT cannot resolve it, OIT will temporarily block access and the student will be referred to Student Affairs.

If issues are not resolved in a timely fashion, OIT is authorized to:

- a. Filter the system’s IP address

- b. Disconnect the system from the network, depending upon the nature and severity of the problem.
- c. If the inappropriate registration involves an IP address owned by ISU, notify the registering agency that ISU owns the IP address, does not approve the registration, and requests that it be removed.

Notice of any such actions will be provided to the responsible parties and units.

Exceptions

Unusual name requests, circumstances, and issues will be referred to the Executive Director, Office of Information Technology for further consideration. Final determination will be subject to the approval of the CIO.

Non-Profit Website Hosting

Indiana State University has limited resources available to meet its computing and communication needs, and bandwidth and maintenance requirements for labor, software, and hardware increase with each website hosted. The purpose of this policy is to preserve these limited resources for support of the University's academic and administrative programs.

Applicability

This policy applies to all faculty, staff, and students who use the Indiana State University network and systems. This policy is applicable to departmental servers as well as OIT servers.

Statement of Policy

- A. Temporary Hosting: Indiana State University systems shall not be used to host a non-profit organization's website on a permanent basis, except in cases that meet the standards noted in the Permanent Hosting section below.
 - 1. Temporary hosting is allowed in the course of developing and testing a website for a non-profit organization as part of an academic assignment. The non-profit organization must also release the University from any liability associated with the hosting before the site is placed on the server. A copy of the current form to be used for this agreement will be posted on the OIT website.
 - 2. Hosting will stop within 60 days of the website's completion. Completion is defined as the time at which ISU student involvement, as a requirement of the course, ceases.
 - 3. At the end of the development and testing cycle, all ISU web servers are to be cleaned of any draft, test, or final components of the website. Components may

include but are not limited to HTML files, graphics, video, sound files, scripts, forms, databases, etc. It is the responsibility of the developers to ensure this is done.

- 4. The permanent hosting of the website and all of its associated components shall be the sole responsibility of the non-profit organization. Long-term hosting issues must be defined and resolved before any ISU website development effort is complete.
- B. Permanent Hosting: Provided the site activity will not unduly impact services, permanent hosting may be granted for those non-profit organizations that have entered into a relationship with ISU that directly benefits the University or one of its programs. That such a relationship exists must be acknowledged by the Chief Information Officer (CIO) before the website hosting is established. Any site existing as of the date of approval of this policy must either verify such relationship through the process below or be removed within 60 days of the approval. Domain names that may indicate a commercial enterprise (e.g. ".com", ".biz") will not be approved.
 - 1. To obtain approval for permanent hosting, the sponsoring ISU department must submit the following to the CIO.
 - 2. Statement explaining how the site's use relates to and benefits the University. Include the name of the ISU employee that will serve as the official liaison to the organization.
 - 3. Technical plan for the website, including name, technical requirements, support requirements, anticipated traffic volume (hits per day, maximum hits in the peak hour, size of files being delivered), and security provisions. The site homepage must include acknowledgment of the University hosting.
 - 4. Content plan for website, including domain name and general content.
 - 5. Signed ISU website hosting agreement. A copy of the current form to be used for this agreement will be posted on the OIT website.
- C. Employee Professional Development: ISU faculty and staff should be permitted web space for professional development or personal purposes. This can include temporary not-for-profit development sites for organizations in which they have an affiliation. Such temporary sites will follow the guidelines in paragraph 3.A with the addition that hosting will be limited to no more than one year. Not-for-profit sites that are to be permanently hosted must be approved as specified in paragraph 3.B. Appropriate agreements must be executed

in either case. When the employee leaves the University, all temporary and permanent pages must be deleted unless responsibility is transferred to another ISU employee. Requests for such transfer of responsibility will be submitted to the CIO for approval.

There are no exceptions to this policy.

INDIANA STATE UNIVERSITY CELLULAR DEVICE POLICY

Reason for Policy – Purpose and Definitions

Indiana State University recognizes that cellular devices are convenient and a feasible alternative for conducting University business. This policy is designed to allow the University to meet IRS regulations by providing guidelines for the use of cellular devices for business purposes. IRS regulations require that the usage of a University-owned cellular device be logged and non-business usage be given a value to either be reimbursed to the University or be included in the user's taxable income. These regulations subject the University and the cellular device user to IRS requirements that are both cumbersome and impractical to fulfill. By shifting the ownership of cellular devices from the University to the employee via additional pay, this policy will eliminate any potential tax compliance issues.

For purposes of this policy, cellular devices are defined as cellular phones, integrated cell phone and email devices (i.e. Blackberries), and other electronic access devices (not including pagers and two-way radios).

Establishment of Business Purpose

With approval and authorization described elsewhere in this policy and where business need justifies the use of cellular access devices, University employees will obtain a cellular device and personal cellular access plan and be reimbursed by the University via additional pay, within an approved pay range. The use of these cellular devices for business purposes can be expensive and the decision to incur such business expenses must be evaluated from a cost/benefit perspective. Departments should consider other viable options such as a landline phone, pagers or other less expensive communication devices when evaluating what type of communication device to use when conducting University business. Additional pay to employees for use of cellular devices must be for business purposes that cannot be accommodated with other less expensive communication devices. Acceptable University business purposes for having cellular devices are:

1. the employee is responsible for emergency University matters where they must be available or,

2. the employee does not have access to a landline phone or other communication device when doing a substantial portion of his or her job or,
3. the use of other less expensive communication devices does not serve as a viable alternative to the business purpose or,
4. the employee's job effectiveness will show a significant increase through the use of a cellular access device or,
5. a group of employees have the need for group or shared devices for purposes such as rotating on-call contact.
6. the responsible vice president determines other legitimate business needs that cannot be served by less costly communication devices. Such purpose must be expressly stated as part of the approval process.

The vice president within each division must approve the issuance of additional pay for an employee who uses these cellular devices. An annual review of the business purpose and associated additional pay must be completed by the department head and approved by the vice president.

Additional Pay for Personal Plans

Employees authorized to receive reimbursement will be paid at a rate of \$50 a month for employees required to obtain a standard phone voice plan and \$90 per month for employees required to obtain a voice and data plan for smartphones such as Blackberries. These rates are subject to annual review and may be adjusted based upon changes in business conditions. The Vice President for Business Affairs and Finance will be authorized and responsible for adjusting these rates after consulting with the University President and the Office of Information Technology. The additional pay is expected to cover maintenance and the replacement of a cellular access device once every 24 months. The additional pay is taxable income subject to payroll taxes and will be included on the employee's W-2 each year.

Base salaries are not to be adjusted to accommodate reimbursement of additional pay and these amounts will not be included in the calculation of percentage increases to base salaries when calculating annual base salary amounts.

Approval Process

Additional pay must be documented using the Cellular Device Additional Pay Authorization Form. This document must be signed by the department head and appropriate vice president in order to substantiate the business need and document the additional pay amount. The completed form should be forwarded to the Payroll Office for payment.

Regardless of when the additional pay amount is established, payments will cease at the end of each fiscal year (June 30).