

SECTION V

GENERAL UNIVERSITY POLICIES, PROCEDURES AND SERVICES

PERSONNEL FILES POLICY

Official personnel files for all faculty members are maintained in the Provost and Vice President for Academic Affairs Office. Executive/administrative/professional staff and support staff official personnel files are located in the Human Resources Office. All official documents concerning personnel actions are to be deposited in the official personnel files.

A faculty member may review the materials in his/her personnel file by requesting a convenient time for that review in the Provost and Vice President for Academic Affairs Office. A member of the executive/administrative/professional staff or support staff may review the materials in his/her personnel file by requesting a convenient time for that review in the Human Resources Office. The materials in the official personnel file are confidential in nature and thus may be reviewed only by the faculty or staff member, by appropriate review committees, and by appropriate administrative and supervisory staff.

Faculty and staff members have the right to respond in writing to any material in the personnel file and to have the response made a part of the file.

Any person wishing to request that any particular item in his/her official personnel file be removed and destroyed may request such action in writing to the University President. The University President will answer all such requests in writing. If the request is approved by the University President, the request and the written approval will be included in the personnel file.

Materials in personnel files will be expunged if the contents violate the employee's civil liberties and if such materials have the potential for inappropriate consideration in future personnel actions. Expunction will occur only upon request of the faculty or staff member and after review and action on the request by the University President.

Personnel Files Contents

All reports, evaluations, assessments, and recommendations will be added to a faculty or staff member's personnel file only with his/her knowledge of that action. A faculty or staff member may examine each and all additions to his/her official personnel file by arranging a convenient time to do so as set forth above.

If and when the University receives an unsolicited paper, the author of which requests confidentiality, the paper will be

returned to the sender with the notation that the University does not retain unsolicited confidential statements about its faculty or staff members.

Anonymously composed letters will be destroyed by the administrator who receives them. Unsolicited oral reports received by an administrator about a faculty or staff member will not be recorded and retained.

The official University personnel file located in the Provost and Vice President for Academic Affairs Office or the Human Resources Office should be a cumulative file of all materials upon which decisions are based at those levels. However, it is recognized that decisions are made in the offices of department chairpersons, deans, and appropriate administrators and that unofficial personnel files will be kept in those places to support such decisions; therefore, cumulative personnel files in those offices shall also be open to employees on the same basis (though not necessarily by identical procedures) as are the official personnel files in the offices of the Provost and Vice President for Academic Affairs and Human Resources. The appropriate administrator at each level will be charged with supervising correct application of the personnel files policy.

Filing Procedures

All personnel records will be in writing and may include electronic records. Materials in the personnel file will be recorded on a register of documents contained in the file. The register will contain:

1. Date on which documents are added to or taken from the file;
2. Title or label of each document;
3. Number of pages comprising each document and any attachments thereto;
4. Source of each document; and
5. Initials of the person making the register entry.

Faculty and staff members will be informed by their supervisor or other administrator whenever documents are placed in their personnel files. (Documents which indicate copy to personnel file satisfy this requirement.) Faculty and staff members have the right to respond in writing to any material in their file; said response shall be attached to the document in question.

Access to faculty personnel files shall be on a demonstrable need-to-know basis for persons formally charged with judging the performance of faculty members in such matters as annual evaluations, promotions, and/or tenure. The responsible administrator shall limit access to personnel files to appropriate administrators and to those persons serving on official personnel committees within the University as attested to by memoranda prepared by an official representative of each such committee.

The responsible administrator will maintain an official record of all persons who view the contents of faculty and staff personnel files. The following information about the reader of each file shall be recorded on a log of readers to be kept in each faculty and staff member's file:

1. Name and position of the reader;
2. Hour and date that the reader received and returned the file;
3. Purpose for which the file was read; and
4. Signature of the reader.

FACULTY AND STAFF PRINCIPLES OF CONDUCT

Indiana State University embraces the values expressed in the following principles. University faculty and staff are:

1. Entrusted with public resources and are expected to understand their responsibilities with respect to conflicts of interest and to respond in ways consistent both with law and with University policy.
2. Expected to be competent and to strive to advance competence both in themselves and in others.
3. Expected to exhibit conduct characterized by integrity and dignity, and such conduct should be encouraged in others.
4. Expected to accept full responsibility for their actions and strive to serve others and accord fair treatment to all.
5. Expected to conduct themselves in ways that foster forthright expression of opinion and tolerance for the views of others.
6. Expected to be aware of and understand those institutional objectives and policies relevant to their job responsibilities, be capable of appropriately interpreting them within and beyond the institution, and contribute constructively to their ongoing evaluation and revision.

RIGHT OF EXPRESSION

The right of expression is as necessary as the right of inquiry and both must be preserved as essential to the pursuit and dissemination of knowledge and truth. Consequently, University faculty, staff and students, individually and collectively, may express their views through the normal channels of communication. University faculty, staff and students also may express their views by demonstrating peacefully for concepts they wish to make known, and the University will make every reasonable effort to protect that right.

It is the objective of the University to provide through explicit reasonable limitations on expression, a context in which expression may be protected and in which violent actions are avoided. The University has an obligation to assure the safety of individuals, the protection of property, and the continuity of the educational process. The following actions are defined as exceeding the limits of appropriate expression or peaceful demonstration and are in violation of University policy:

1. Actions which endanger the safety and well-being of individuals.
2. Actions which destroy property.
3. Actions which disrupt, by physical or auditory means, the on-going operations of the University or interfere with the rights of other individuals in their exercise of expression.

Individuals holding views opposed to those presented by persons participating in a peaceful demonstration, protest, or other expression of attitudes are subject to the same policies.

NEPOTISM

Faculty and staff may not participate in decisions affecting the appointment, tenure, promotion, or other personnel actions involving a relative. In situations where direct supervision by a relative is involved, the next level supervisor will be responsible for establishing procedures as required to assure equitable personnel decisions.

For purposes of this policy, a relative is defined as parent, spouse, child, brother, sister (including in-laws), and other close relatives by birth or marriage (such as aunt, uncle, nephew, or niece).

IDENTIFICATION CARDS

All students, faculty, and staff, including temporary and courtesy appointments, are required to have an identification card in their

possession at all times while on campus. This card is used for University functions. Identification cards are issued by the Public Safety Office. New students, faculty and staff are not charged for the first identification card; however, there may be a fee for replacement cards.

All card types may be obtained directly from the Public Safety Office with the exception of the recreational sports identification card. A form indicating ISU staff or guest user must be obtained from the Recreational Sports Office and presented to the Public Safety Office. Payment for the card, if required, and any fees assessed for facility/equipment services usage must be submitted to the Recreational Sports Office when the form is completed.

BUILDING KEYS

University keys are issued by Facilities Management, Hulman Memorial Student Union, Residential Life Office, and Hulman Center based upon the following guidelines.

1. Requested keys must be properly authorized as follows:
 - a. Building master keys--authorized by the appropriate vice president.
 - b. Sub-master building keys--authorized by the appropriate dean.
 - c. Individual and outside door keys--authorized by the appropriate department head or chairperson.
2. Keys must be picked up and signed for by the individual using the key, indicating the acceptance of responsibility for and proper use of the key.
3. University keys may be duplicated only through the Facilities Management Office upon appropriate authorization.
4. University keys may not be loaned to unauthorized personnel. Proper identification shall be required from any individual before any key is loaned out by any University office.
5. In the event a key is lost, it may be replaced by proper authorization at a nominal cost to be paid at the Controller's Office by the person to whom the key was issued. In the event it becomes necessary to rekey an individual lock, the individual will be charged actual University costs.
6. Access may be gained to University buildings after hours by contacting the Public Safety Office.
7. Persons leaving University employment must return all issued keys prior to issuance of the final pay check. Keys will be returned to the issuing office or left with the Human Resources Office during the exit interview.

USE OF UNIVERSITY SUPPLIES AND EQUIPMENT

University faculty and staff are prohibited from using University equipment and supplies, including computers, printers, telephones, copy machines, etc., for non-university related business or organizations. The unauthorized use of University property is considered conversion under the State of Indiana Criminal Code 35-43-4-3.

University owned equipment is to remain on the premises of Indiana State University and is not to be removed or taken home. Equipment may be removed from University property for the purpose of making presentations, or for fieldwork in remote locations, if approved by an immediate supervisor. Laptop computers and portable devices may be an exception and may be taken home, provided the equipment travels back and forth to work with the employee.

Any equipment, which a department can no longer use, should either be transferred by intramural voucher to another department that can use the equipment, or the equipment should be declared surplus and arrangements should be made with the Purchasing and Central Receiving Department to pick up the equipment. All surplus equipment retained by the Purchasing and Central Receiving Department is available for use by other University departments. If there is no interest or use for the surplus equipment at ISU, the equipment is sold or disposed of by the Purchasing and Central Receiving Department, usually at a public auction or through a competitive bidding process.

MOTOR VEHICLE AND TRAFFIC REGULATIONS

Faculty, staff and students who bring vehicles to campus will be held responsible for the registration and proper operation of their vehicles. It is the responsibility of each member of the University community to read, understand, and abide by the motor vehicle and traffic regulations. Ignorance of the regulations is not an acceptable reason for appeal of a violation.

Parking permits are required and may be purchased in the Traffic and Parking Services Office. Fees are determined annually. Faculty and staff may elect to purchase parking permits through payroll deduction either before or after taxes. The complete motor vehicle traffic and parking regulations are presented in Appendix D.

NON-MOTORIZED VEHICLES

Policy

Indiana State University recognizes Non-Motorized Vehicles are important and legitimate means of transportation provided they are operated with due regard and concern for the safety of the general public. Non-Motorized Vehicles may be operated on campus sidewalks and paths provided they are used solely as a means of transportation and not for purposes prohibited by this regulation. Pedestrians in all locations designated for pedestrian traffic shall have the right-of-way over Non-Motorized Vehicles.

Definition

For purposes of this regulation “Non-Motorized Vehicles” shall include: Bicycles, Tricycles, Unicycles, Skateboards, Roller Skates, In-line Skates, and any other human powered transportation device.

Prohibited Activities

Non-Motorized Vehicles shall not be operated:

1. In a reckless or hazardous manner;
2. In a manner that is unreasonable for existing conditions;
3. In a manner that interferes with pedestrian or vehicular traffic;
4. Inside University buildings;
5. On ramps established for the use of persons with disabilities;
6. Immediately adjacent to building doors;
7. On stairs, railings, landings, loading docks, benches, picnic tables, and all surfaces not intended for pedestrian or vehicular travel;
8. In areas posted against their use;
9. In an acrobatic or stunting manner, i.e. activities causing one or more sets of wheels to leave the ground or other surfaces intended for pedestrian or vehicular travel.

Exception

Nothing in this regulation shall prohibit the operation of Non-Motorized Vehicles consistent with any authorized University activity.

Penalties

1. Non-Affiliated Persons
 - a. First Offense – Receive a verbal warning. A record of this warning shall be kept on file at the Public Safety Dispatch Center.
 - b. Second Offense – Issue “No Trespass” directive from University property.
 - c. Subsequent Violations – Arrest for Trespass.
2. Faculty, Staff, Students, and other persons affiliated with the University
 - a. First Offense – Receive a verbal warning. A record of this warning shall be kept on file at the Public Safety Dispatch Center.
 - b. Subsequent Violations – Be issued a campus traffic ticket charged with “Other Moving Violation” and fined \$20.

FACULTY/ STAFF TRAVEL

Indiana State University enables employees of the University to be reimbursed for actual and necessary travel and other expenses incurred while on official business, if approved by the University. Persons who travel on University business are encouraged to incur the lowest practical and reasonable expense while still traveling in an efficient and timely manner. Those traveling on University business are expected to avoid impropriety, or the appearance of impropriety, in any travel expense. They must conduct University business with integrity, and in compliance with University travel guidelines and procedures. The University travel guidelines and procedures can be found at <http://web.indstate.edu/controller/finance/travel-bud/home.html>. These guidelines are approved with action of the University Board of Trustees on December 3, 2004, and periodically revisited to ensure consistency with various tax laws and regulations.

FLAG GUIDELINES

The Public Safety Office is responsible for the display of the national, state and other appropriate flags on official university flagpoles.

1. Upon the death of a member of the faculty or staff, as an employee of a state institution, the state flag will be draped and flown on the day of the funeral.

2. Upon the death of a student enrolled at Indiana State University, the University flag will be draped and flown on the day of the funeral.
3. Fraternal groups may request that their flag be flown on their national founder's day with the American flag. Such permission is sought through the Vice President for Student Affairs Office. The organization will be responsible to provide the flag to the Public Safety Office by 4:00 p.m. the day prior to the founder's day.
4. If on the same day, two (2) separate requests are made to fly two (2) separate organizational flags, each flag will be flown half a day.
5. No flag, including the American flag, may be displayed on official university flagpoles except with the approval of the Public Safety Office.

USE OF UNIVERSITY FACILITIES

The University has established policies and procedures for maximum benefit and utilization of its resources, facilities, and services. The policies and procedures include safeguards and administrative guidelines, and define the University's obligations to matriculated students, the faculty, the staff, and the public.

Reservations for meeting rooms in campus buildings other than Hulman Memorial Student Union, Tirey Hall, and Hulman Center may be made on forms available in the Registrar's Office. Groups not associated with the University may be charged a rental fee for the use of University rooms at established rates which are available in the Controller's Office.

Student activities space of a general nature is available in Hulman Memorial Student Union, Tirey Hall, and Hulman Center. Space for social events, such as dances, movies, organizational meetings, and other activities, will be reserved through the director of the facility.

The facilities of the University include all buildings and grounds owned or leased by the University. Space within the buildings and grounds is of three types: dedicated, semi-public, and public.

Dedicated

Dedicated space is defined as space used primarily to serve and support the educational, cultural, residential, and recreational functions of the University. Although such areas may be used by the public, University functions have priority. Examples of such space are: classrooms, laboratories, libraries, residence halls, parking areas, recreational facilities, intramural and athletic fields.

Semi-Public

The semi-public space areas are defined as space available for use by internal and external individuals and groups on a reservation only basis. Normally, non-University organizations will pay a rental fee for the use of such space. Examples of such space are: Tilson Music Hall, activity and meeting rooms in Hulman Memorial Student Union, Tirey Hall, and Hulman Center.

Public

The public space areas are defined as those which accommodate pedestrian as well as vehicular traffic flow and facilities of the University open to the public. These areas are defined to include sidewalks, campus streets and drives, entrances to buildings, lobbies and corridors in classroom and office buildings and semi-public facilities, and commons areas in the residence halls, Hulman Memorial Student Union and Tirey Hall.

Guidelines

1. Every person with legitimate business at the University has the privilege of access to the public areas of the buildings and grounds during designated open hours.
2. Soliciting for monetary reasons or selling will not be permitted on the campus except in cases of student groups whose activities are approved through the Student Affairs Office.
3. Use of space for purposes other than those for which it has been designated will not be allowed. Neither will individuals or groups be permitted to interrupt the use of space after it has been duly assigned, without permission of the University President or designee.
4. Space in lobbies which are designated public areas as defined by this policy may be reserved by recognized student, faculty, or staff organizations. Public groups, organizations, or agencies may reserve these areas for purposes other than recruitment for employment, or which are intended to culminate in recruitment for employment, if approved by the designated building coordinator. A listing of building coordinators is maintained in the Risk Management Office.
5. The University reserves the right to deny the use of areas if it is determined that access by the group is disruptive to the normal operation of the facility or the University. If the individual in charge of a facility or function determines a situation is no longer peaceful and orderly, the assistance of the Public Safety Office will be requested.

6. Agencies coming to campus to recruit full-time employees must make reservations for space and schedule with the Career Center. The Center will schedule personal interviews in its facilities or in semi-public areas if the facilities of the Center do not accommodate the demand.
7. Agencies wishing to recruit near a heavy traffic area may reserve a room at a regularly established rental rate. Reservations for facilities must be made with the person responsible for the building in which the space is located.
8. Agencies coming to campus to recruit students for part-time or temporary employment may make reservations for space with the student employment staff in the Human Resources Office.

University Groups and Agencies

Employee groups and officially recognized student organizations may schedule University facilities on a space available basis for the purpose of holding meetings or conducting activities consistent with the objectives of that organization. Use of any facility is determined by the University officials designated by the University President according to the following priorities.

Permanent Academic and Office Space

Academic department chairpersons will submit requests for space needs of a permanent nature, such as faculty offices, research, and instructional laboratories, to the appropriate academic dean's office. All such requests will then be forwarded to the Provost and Vice President for Academic Affairs Office.

General Instructional Space

General classroom areas in the academic buildings are not assigned to any specific academic department. These areas are under the jurisdiction of the Registrar's Office for assignment of regularly scheduled classes and are available for meetings and study purposes only on a temporary basis.

General instructional space other than classrooms, such as tennis courts, athletic fields, the ISU field campus, and library study rooms, may be reserved for use by making application to the specific department to which the desired space has been assigned.

General Buildings and Grounds

Persons with legitimate University related business have the privilege of access to the public areas of the buildings and grounds during designated open hours. These areas are defined to include sidewalks, certain designated streets, entrances to buildings, corridors in classroom and office buildings, library reading rooms, and commons areas in the residence halls,

Hulman Memorial Student Union and Tirey Hall.

The University President, or designee, may deny access to an individual or group which disrupts the normal operation of the University.

Non-University Groups and Agencies

The University recognizes its obligation to extend its facilities to its communities-at-large under that same priorities and guidelines followed by University groups. These resources bring together students, scholars, and the public in educational and cultural settings. University projects concerned with the resolution of societal, environmental, business, or industrial problems often involve students, faculty, and representatives of the communities-at-large to mutual advantage.

Conferences and Special Events

The Center for Public Service and Community Engagement is responsible for scheduling and managing conferences held at Indiana State University and provides assistance in the major areas of conference planning and implementation.

VISITING SPEAKERS

Indiana State University considers freedom of inquiry and discussion essential to a student's educational development. The appearance of visiting speakers is encouraged as one means by which members of the University community are provided with an opportunity to explore a variety of views and opinions.

The University recognizes that any subject or view may be repugnant or distasteful to an individual or group holding divergent views. The University further recognizes that the question of appropriateness is not determined by the subject matter as such, but by the method of presentation and the extent to which there is critical examination through disciplined inquiry by faculty and students.

Restraints on activities connected with learning should be held to that minimum which is consistent with preserving an organized society in which peaceful, democratic means for change are utilized. Each individual has the right to express ideas and opinions; however, it must be recognized that those who have different opinions have the same rights. The exercise of rights involves acceptance of responsibility.

On the basis of these premises, Indiana State University will encourage any University recognized group of students, faculty, or staff, to invite speakers to campus subject to the following guidelines.

Guidelines

1. The speaker does not advocate violation of any federal or state law.
2. Following the speaker's presentation, adequate time should be allowed and opportunities provided for questions and comments from members of the audience. The speaker must be made aware of and agree to this condition.
3. Neither the sponsoring group nor the speaker will indicate University support of the speaker or his/her ideas.
4. A member or members of the sponsoring group will be in attendance with the speaker to present the speaker and the topic as well as to conduct the question period.
5. In order to properly schedule the event, assure adequate facilities, ensure necessary publicity and proper procedures, the sponsoring group wishing to invite a visiting speaker to the University will make all reservations of space with appropriate University officials seven (7) days in advance of the speaker's appearance.
6. Approval for visiting speakers may be obtained from the appropriate University office as follows:
 - a. Office of the Provost and Vice President for Academic Affairs--faculty, administration and staff.
 - b. Office of Student Life--SGA, fraternities, sororities, Union Board, and all other student organizations (departmental, honorary, religious, etc.).
 - c. Office of Residential Life--residence halls and organizations.
7. Speakers participating in regularly scheduled classes or University programs or speakers seeking state or federal offices are covered under other provisions. (See also University Handbook, Section III, "Methods of Instruction," and Section V, "Political Activities".)

WEATHER GUIDELINES

Although weather conditions may necessitate the closing of the University, such occasions are extremely rare. The University's academic programs, courses, classes, seminars and offices will continue and remain open, except in the most unusual circumstances.

When a decision is made to close the University--that is, a decision to cancel classes and to close University offices--an official announcement will be made by means of radio and

television reports. When information is not conveniently available through public news media, verification of the University's status is available on the ISU Infoline (237-7777).

The decision to close the University because of weather conditions will be made by the University President, or designee. When a decision is made to close the University because of weather conditions, certain institutional services must continue on an emergency basis. When possible, services at the following locations will be continued:

1. University Arena
2. Student Health Center
3. Facilities Management (designated staff)
4. University Power Plant
5. Residence Halls
6. Public Safety Office

Supervisors of these services are responsible for maintaining sufficient staff in such circumstances. Activities scheduled for Hulman Memorial Student Union and Hulman Center may require University staff coverage. Facilities for plant and animal research will be staffed by the appropriate departments. Additional emergency needs will be addressed and responded to by the appropriate vice president.

When a tornado has been sighted which places the campus area in danger, a siren will be sounded. All persons on campus should immediately move inside and go to shelter areas designated on emergency procedures signs posted in campus buildings. In general, the best shelter is below ground level or in lower interior areas of reinforced concrete buildings out of sight of windows and glass doors.

Persons responsible for offices, laboratories, and other facilities should develop procedures for securing facilities against theft during a severe weather warning or drill.

PUBLIC RELATIONS

The maintenance of good public relations is important to the welfare of the University. The following guidelines should be observed in promoting and preserving the best interests of the University.

1. Neither the University name nor an individual's title should be used in discussions of public controversial issues.
2. University letterheads, return envelopes, postage, or an individual's title should be used only in professional correspondence.
3. Charging for personal services other than services commonly associated with one's employment is an individual matter. However, tact and judgment should be

exercised in the interest of community and public relations. Should charges be made for services rendered, the services should not be performed on campus or on "school time" (the time necessary in the satisfactory fulfillment of the individual's assigned responsibilities).

4. Departments of the University charging off-campus individuals or groups for services of the department must have the approval of the appropriate vice president. Arrangements for handling funds received for such services should be made with the Controller's Office. See also University Handbook, Section V, "Sponsored Programs", "Professional Consultant Service", and "Outside Work or Other Employment".

Political Activities

Indiana State University, as a public educational institution, must necessarily be nonpartisan in all of its political and governmental relationships and does not support any political party or candidate for public office. Members of the staff who participate in political activities, support candidates, or become candidates for public office, do so as individuals and, as such, must not use the University facilities, the University name, or involve the University in any way in connection with such activities. Political parties or organizations may use University facilities for meeting purposes on a rental basis the same as other civic and social organizations or groups. Such use, however, does not in any way imply that the University sponsors or supports the organizations, their purposes, or their programs.

Governmental Relations

In conducting the official business of the University, it is necessary to deal with many state and local governmental officials and the state legislature. The Governor and the legislature of Indiana are responsible for and have authority over many aspects of the University operation. University business must be conducted through the Indiana Commission for Higher Education, the State Budget Agency, the State Auditor, the State Treasurer, the State Board of Accounts, and other state officials and boards. These relationships are conducted by the University President, or designee, as authorized by the ISU Board of Trustees. Unless authorized by virtue of his/her official position or by designation as a representative of the University by the ISU Board of Trustees or the University President, no member of the faculty or staff may speak officially for the University or enter into any negotiations which involve commitments or obligations on the part of the ISU Board of Trustees or the University administration.

News Releases

General University news and professional activities of faculty and staff are announced to the public through news releases prepared and distributed to the various media by the Public Affairs Office. Faculty and staff are advised to cooperate with that office in making the necessary information available for release.

Actions by the Indiana State University Board of Trustees are announced by the President of the Board or by the University President through the Public Affairs Office.

Campus Solicitations

No canvassing, selling, or soliciting by outside individuals or organizations is permitted on the grounds or in the buildings of the University without the written permission of the University President. Any solicitation activity or violation should be reported to the Public Safety Department.

Commercial Advertising

The University does not lend its name to the advertisement and endorsement of commercial enterprises and products. Advertisement in University publications and activity programs does not imply official endorsement.

FUND RAISING FROM PRIVATE SOURCES

The University President is the official spokesperson in all fund-raising activities. The Vice President for University Advancement, in concert with the other administrative units of the University, will assess University needs, identify possible private sector sources for funds to meet those needs, prepare plans for soliciting private sector funds and direct the personnel and financial resources available toward obtaining resources to meet those needs. All University efforts in private sector fund raising will be coordinated through the University Advancement Office.

PURCHASING PROCEDURES

The Purchasing and Receiving Department has been charged by the Board of Trustees with the responsibility for the procurement of all materials, equipment, supplies, and contract services; of warehouse operations; and of disposal and sale of surplus materials and equipment. Additionally, the Board of Trustees has authorized purchases by University Departments that use the ISU procurement card, provided the established rules for the procurement card program are followed. The

procurement card procedures can be found at (<http://www.indstate.edu/purchasing/>).

The Purchasing and Receiving Department has the sole authority to order materials, equipment, etc., and obligate the University for same, except for purchases made through the procurement card program. Any orders, whether written or verbal, will be recognized only if authorized by or through the Purchasing and Receiving Department, or as a result of the proper use of the procurement card system.

Procurement shall be conducted according to Indiana Statutes 5-22-16-4, 6-2.5-4-14, and 6-2.5-8-10, which requires that state educational institutions provide the State of Indiana with vendor lists, in order to determine if vendors have a registered retail merchant certificate and are not delinquent in paying gross retail and use taxes.

The following items are not routinely handled by the Purchasing and Receiving Department:

- Real estate
- Books and other holdings for the libraries
- Utilities (water and electricity)
- Insurance and contracts for professional services
- Contracts signed on behalf of the Board of Trustees
- Travel
- Legal investments and bond underwriting

The policies and guidelines outlined in Appendix F have been approved by the University Board of Trustees and are intended to assist the faculty and staff in understanding the procedures and responsibilities of the University Purchasing and Receiving Department. Since these policies and procedures are designed to serve the interests of the departments, as well as to meet policy requirements of the University, faculty and staff are expected to give full support and cooperation. It is recognized that problems and misinterpretations of regulations may occur. In such instances, departments are urged to discuss such problems with the Purchasing and Receiving Department.

UNIVERSITY LETTERHEADS AND ENVELOPES

Letterheads, envelopes, and business cards used by individuals, departments, centers, offices, schools, or other units of the University should be uniform in wording, type style, size of type, and layout. The approved formats are provided by the Division of Printing. The Purchasing and Central Receiving Department will not accept purchase orders for these items to off-campus vendors.

CONTRACT APPROVAL, SIGNATORY, AND REPORTING POLICY

The approval, signatory, and reporting policy relating to contracts is designed to ensure greater continuity in the way contracts are handled, control over contract negotiations, safeguarding of the interests of the University by assuring regulatory compliance and fiscal protection, and more efficient internal processes.

This policy operates to delegate contract power vested in the ISU Board of Trustees by statute to others. The University President and University Treasurer may further delegate any authority they may possess to approve or execute a contract, but such delegation must be in writing, and may only be made to a vice president or to the controller. This policy shall be construed in conjunction with the University Purchasing and Receiving Policies and Procedures.

As a state supported institution of higher education, the University is exempted from most of the purchasing requirements applicable to state agencies, with the exception of purchasing preferences relating to equipment, goods, and materials. Therefore, with regard to the purchase of goods and supplies in the daily operation of the University, the University is bound to follow the purchasing preferences set forth in the Indiana Code, and bound to adhere to its own purchasing policies.

Authority to contract for professional or expert services, for new construction projects, to rehabilitate or repair capital facilities of the University, and to bond such projects is covered under a variety of Indiana statutes, and special rules apply to these situations. Special rules also apply to transactions relating to real estate, including leases, and to any transaction that would involve a sale of University assets. Individuals with responsibility for these projects shall communicate and coordinate with University Counsel and the University Treasurer. Individuals are strictly prohibited from altering State property without appropriate approval.

Indiana law vests authority in the ISU Board of Trustees to approve any student fees, other fees, bonding, and issues relating to compensation and benefits of University employees. University employees are strictly prohibited from implementing any fees, bonding, or making any determinations relating to compensation and benefits that are not first expressly authorized by the ISU Board of Trustees.

Individuals representing the University should remember that contracts to which the University is a party can generate revenue for the University, as well as bind the University to an expenditure. Institutional concerns include assurances that the contract is appropriately negotiated, fits within the academic

mission of the University, and that the University possesses the resources necessary to complete requirements under the contract. All contracts must have an attached routing form that is completed before the signatory can execute the contract. No routing form can be altered in the approval process; all comments in the approval process shall be reflected on the routing form for purposes of reference. In any contract that binds the University to an expenditure of funds, the University Treasurer, or designee, must sign the routing form prior to execution of the contract.

Contracts commonly entered into by the University, listed by category, with approval and signatory assignment are indicated in the detailed policy available in the University Legal Affairs Office. All contracts entered into that do not require ISU Board of Trustees' approval are required to be reported at the ISU Board of Trustees' meeting following the date upon which the contract is entered into, with the exception of contracts falling under the University Purchasing Policy, which contains other reporting requirements.

UNIVERSITY PUBLICATIONS

Requests for the printing of University-wide publications should be initiated in the University Publications Office which provides funding for schedule bulletins, catalogs, and for student recruitment publications for the Admissions Office and academic departments within the colleges (with approval of the chairperson or dean and the Director of University Publications). This funding is for publications which the University Publications Office coordinates. Other publications are funded by the initiating department or office. The University Publications Office assists in the production of all publications, regardless of which unit expends the budget. The University Publications Office provides professional writing, editing, design, and layout services and, when needed, will also coordinate photography.

Brochures, bulletins, and other materials giving information about University programs, services and activities are prepared and distributed by the University Publications Office.

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").

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.

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).
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). Therefore, department heads must annually review documentation to ensure that a business purpose continues to exist and submit a new Cellular Device Additional Pay Authorization Form to the Payroll Office at the beginning of each fiscal year in order to continue the additional pay. Termination of the additional pay is required if the business purpose no longer exists.

The department must have documentation that proves the employee actually obtained the device (i.e. phone number of cell phone). Full accountability for the appropriateness and reasonableness in amount of the additional pay for the devices covered in this policy are the responsibility of the department head and responsible vice president.

Employee Use of Cellular Devices

The employee may use the phone for both business and personal purposes and may, at his or her own expense, add extra services or equipment features as desired. Because these devices are the property of the employee, cellular devices that are lost or damaged are the responsibility of the employee to promptly replace.

Use of the cellular device in any manner contrary to local, state, or federal laws will constitute misuse, and will result in immediate termination of the additional pay.

Unavoidable Business Costs Associated with Non-Typical Use

Extraordinary cellular charges (such as out of country roaming charges) incurred due to a legitimate business need may be presented with appropriate documentation as reimbursement of travel expenses subject to the approval of the University Treasurer or his or her designee.

Cellular Devices Remaining on University Contracts

Some departments have multiple staff sharing a single device for on-call rotations and designated departments have been issued a cellular device in the event of a disaster. For these reasons, a number of shared or group devices will remain available via University contracts. Personal calls or contacts are not to be made to/from these devices. No department in the university can extend existing cellular contracts or enter into any new contracts with cellular companies, except the Office of Information Technology.

Grants and Contract Accounts

On federal or federal pass through Grants and Contract Accounts only shared or group devices will be allowed. The only use of cellular devices on Grants and Contract accounts are those which have allocated funds to be directed to the Office of Information Technology and an approved University contract established. In these cases, the use of the cellular device should be fully devoted to the project, necessary for the project, and included in the approved budget. In cases where it is not in the approved budget, the expense will not be allowable unless approved by Grants and Contract Administration. The bona-fide business purpose documentation must be approved annually by Grants and Contract Administration in order for the expenses to be allocable to a Grant and Contract Account. Personal calls or contacts are not to be made to/from cellular devices approved under this section.

Indiana State University Foundation Accounts

Direct payment for cellular phones or other electronic devices is not allowable on Indiana State University Foundation accounts.

Testing Exclusion

The Office of Information Technology is excluded from this policy where it needs to continue existing or establish new University contracts or acquire electronic access or access devices for testing or to support University information services for such testing devices. Such exclusions shall only be approved by the Chief Information Officer who is responsible for monitoring eligibility and use. The use of these devices are

for testing purposes only and personal calls or contacts are not to be made to/from these devices.

Future Service

The Office of Information Technology may provide a service to maintain a small number of cellular access device contacts for organizations that have multiple employees sharing a single device for on-call rotations. No personal calls or contacts are to be made to/from these devices.

SPONSORED PROGRAMS

Proposals Externally Funded

The University encourages faculty and professional staff to seek external support for research and creative projects. External sponsors often provide support for release time, personnel, equipment, travel, and expendable supplies. Because such activities affect the department and often require naming the University as the applicant, rather than the faculty member, all proposals submitted to external agencies or individuals must be approved by University departments/offices affected by the proposed project. These approvals are obtained by routing the proposal through the steps outlined on the University Routing Sheet and in the pamphlet titled "Preparing and Routing a Grant Proposal at Indiana State University", both of which are available in the Sponsored Programs Office. This procedure assures coordinated effort and consistent reporting once the proposal is funded.

To facilitate the development and submission of proposals for external funds, the following procedural steps have been established:

1. Faculty members contemplating the preparation of proposals should contact the Sponsored Programs Office. This Office provides valuable information about funding opportunities and has a proposal development specialist to assist with the writing and a grant account specialist to assist with the budget. Seeking assistance while writing early drafts may eliminate potential problems in the routing process once the final draft is completed. It is also important for faculty and staff to discuss ideas with supervisors and any colleagues who might be involved with or affected by the project.
2. The prescribed format will usually be set forth in the agency's guidelines and application materials, and some agencies request special forms. The Sponsored Programs Office can aid in the preparation of a targeted, well-organized, well-written, specific proposal and provide

assistance and institutional information needed to complete sponsor forms.

3. A current University Routing Sheet should be obtained from the Sponsored Programs Office. Use of outdated forms may impede the routing process. Completed, typed proposals should be routed at least ten (10) days prior to the anticipated date of posting/delivery.

The University Routing Sheet should be circulated with one (1) complete original (or the number requiring original signatures) and two (2) additional complete copies which will be retained in the Sponsored Programs Office. These materials are to be circulated in the order listed below under "University Compliance Committees" or other applicable compliance committees; chairpersons of all departments affected by the proposed project; deans of all colleges affected by the project; and the Provost and Vice President for Academic Affairs Office for final review and approval.

4. When all aspects of the proposal are in order, the Sponsored Programs Office forwards the proposal to the grants and contracts administrator in the Controller's Office for budget approval. It is then forwarded to the Provost and Vice President for Academic Affairs Office for final approval.
5. All proposals must be signed by the Provost and Vice President for Academic Affairs or the appropriate vice president.
6. When all signatures have been obtained, the Sponsored Programs Office will contact the faculty or staff member for mailing of the proposal.

Externally funded or contracted projects will be in an amount agreed upon by the University and the sponsoring agency. Time spent on contract research or sponsored instructional activities will be reimbursed to the University out of contract funds, and the faculty and/or staff member will normally be paid no more than his/her established University salary during the academic or fiscal year. In no case will a faculty member be paid more than 120 per cent of his/her academic year salary when participation in such research or instructional assignment is added to the regular academic year assignment. During the summer, a faculty member may earn no more than 30 per cent of his/her academic year salary.

University Compliance Committees

Indiana State University acknowledges its responsibility to assure scientific and ethical research and to comply with federal mandates. The University has established compliance committees and filed appropriate assurances with the U. S.

Department of Health and Human Services. These committees include:

Institutional Review Board for the Protection of
Human Subjects
Institutional Animal Care and Use Committee
Radiological Control Committee
Institutional Biosafety and Recombinant DNA Committee
Environmental Safety Committee

Proposals requiring special approval from one or more of these committees should be routed to the chairperson of the respective committee(s) for approval prior to routing to the department chairperson(s). Further information on these committees is available in the Sponsored Programs Office.

Human Subjects Research

Research projects involving the use of human subjects must be approved by the college in which the research project is located. The ISU Institutional Review Board for the Protection of Human Subjects must review and approve external research proposals and may be asked to review internal proposals. Once approval has been granted, it is unacceptable to deviate significantly from the approved protocol without again obtaining approval. It is also improper to violate the confidentiality of a human subject without the subject's approval.

A manual, "Policies and Procedures for the Review of Research Involving Human Subjects", has been prepared to assist all members of the University community in complying with the stated policy of ISU with respect to external and internal research involving human subjects. The attention of the researcher is especially drawn to the code of ethics adopted by the various behavioral sciences professional organizations.

PROFESSIONAL CONSULTANT SERVICE

Professional consultant service is a proper contribution of a university to the public which supports it. The following statements of policy are designed to ensure the quality of such professional activity and provide adequate protection for both the interests of the University and those faculty and staff who engage in professional consultation.

1. Faculty and staff are encouraged to participate in consulting activities appropriate to their academic or professional areas of competence.
2. Consulting activities should not involve absence from the University for more than 20 per cent of the total time committed to the regular work week. Consultation must

neither be in conflict with, nor detract from, the faculty or staff assignment at the University.

3. Expenses for consulting activities will be supported by the University only if the faculty or staff member carries on the tasks as the official representative of the University and has been approved to do so by the University President or an authorized representative.
4. Faculty and staff engaging in consulting activities must inform the department head of the commitment of time involved prior to acceptance of the obligation. The Consulting Service Report Form is to be used for this purpose.
5. If the faculty or staff member has entered into a consulting relationship with an agency on his/her own initiative, the University liability under the Indiana Workers Compensation Act does not provide protection to the faculty or staff member when thus engaged.
6. Consultation fees are determined by mutual agreement between the person or agency requesting service and the faculty or staff member of the University department/office offering the service. Fees shall not be charged for internal consultation within the University, except in those instances where the activity is funded from outside sources. The faculty or staff member will normally be paid no more than his/her academic or fiscal year salary, and in no case, more than 120 per cent of his/her salary when such assignment is added to the regular assignment. During the summer, a faculty member may earn no more than 30 per cent of his/her academic year salary.

OUTSIDE WORK OR OTHER EMPLOYMENT

Regular appointments to the faculty and professional staff require full-time service to the University. Commercial activities, private employment, or other outside work for remuneration should not be undertaken without prior authorization. Such activities must not conflict with the performance of the University assignment. Should such assignments require absence from work during the regular work schedule, vacation, if applicable, or leave without pay should be used.

Only under unusual circumstances will there be extra compensation for fiscal year professional staff paid from funds managed by ISU. Such extra compensation requires the approval of the appropriate vice president. Approval must be granted before the project or activity is undertaken.

INTELLECTUAL PROPERTY POLICY

Indiana State University is committed to the scholarship, research, creative, and other academic and service activities of its faculty, librarians, staff, and students. By virtue of its mission, employees and students of the University will naturally produce new written works, inventions, works of fine and performance art, discoveries, new or improved products or processes, ornamental designs, compositions of matter, multimedia materials, new varieties of plants, and many other expressions of learning, research, and scholarly activity. These works may, and often involve rights of ownership, needs for protection, rewards from ownership, and responsibilities during development that affect all individuals involved and the University as a legal entity. The Intellectual Property Policy appears as Appendix J.

UNIVERSITY ARCHIVES

The University Archives is the designated repository for official records of Indiana State University. The purpose of the Archives is to preserve materials having intrinsic historical, legal, evidential and/or administrative value to the University, thereby providing useful documentation of the people, policies, and events in its history. The Archives constitutes the most significant and steadily growing resource for research at all levels into the history of the University community, provides a means of accountability in its governance, and serves as a basis for continuity in its administration.

The Archives contains a body of publications, theses, minutes, correspondence, student records, personnel records, photographs, financial records, and faculty publications dating back to the earliest years of the Indiana State Normal School. The use of these materials is subject to restrictions stipulated by the depositor, whether official or private.

The University Archives Committee advises the University President and other officials of the University in records policy administration. Advisory responsibilities are to codify statements of policy for the University Archives and to revise the policies when necessary. The University Archives Policy is contained in Appendix G.

COMMUNICABLE DISEASES

It is the intent of Indiana State University to assure that all reasonable steps will be taken to discourage the spread of communicable diseases within the University community, especially those diseases which may be considered life-threatening. Within the communicable diseases category are a wide variety of infectious illnesses which range from the common cold to the Acquired Immune Deficiency Syndrome (AIDS). Such diseases vary greatly in mode and ease of

transmission, the seriousness of effects and in the means to prevention and treatment.

All units of the University have the responsibility to promote sound health practices through educational programs, to assist persons who may have health problems to receive proper attention, and to exercise special care when communicable diseases are suspected of being present.

Individuals who have, or suspect that they have, a communicable disease are encouraged to seek and to follow the best medical advice available. The Student Health Center will observe professional practices of care and confidentiality in regard to patients served and will comply with the reporting requirements of all public health agencies. If there are occasions when special dangers of contagion require unusual actions by any part of the University, such actions will be as a result of recommendations by the Director of the Student Health Center to appropriate officials of the University.

The University seeks to discourage the spread of communicable diseases through programs of education and awareness, prevention and early detection, and special care. The privacy, rights and confidentiality of all individuals will be respected, and the University will comply with all federal, state and municipal regulations.

Bloodborne Pathogens Exposure Control Plan

The University has developed a program to protect faculty, staff and students who have occupational exposure to blood and other potentially infectious materials. This program, the ISU Bloodborne Pathogens Exposure Control Plan, complies with the requirements of the OSHA Bloodborne Pathogens Standard, 29CFR 1910.1030, the Indiana Administrative Code 410 IAC 1-4 and identifies procedures to eliminate or reduce the risk of contracting a bloodborne disease in the workplace. A copy of the Bloodborne Pathogens Exposure Control Plan is available in the Environmental Safety Office.

The Bloodborne Pathogens Exposure Control Plan applies to all employees of Indiana State University, including part-time and temporary staff, who may as a part of their employment come into contact with blood, infected lab animals, or other potentially infectious material.

Health care and laboratory employees whose work may involve the risk of exposure to blood or other potentially infectious materials may include, but are not limited to, the following: physicians, nurses, nurses aides, physician assistants, phlebotomists, medical technologists, therapists, research laboratory personnel, research scientists, and animal laboratory personnel.

Others whose positions may include some occupational exposure tasks include employees in law enforcement, custodial/housekeeping services, laundry services, maintenance, child care, equipment technicians, transportation service workers, or couriers involved in delivery and transport of potentially infectious materials.

Universal precautions refer to approaches to infection control in which all human blood and certain human body fluids are treated as if known to be infectious for HIV, HBV, HCV or other bloodborne pathogens. Using this assumption when dealing with infectious materials eliminates the need for decision making to determine the extent of actual or potential disease hazards. The

approach establishes minimum standards for contamination control that will effectively control bloodborne pathogens if present. Universal precautions shall be observed to prevent contact with blood or other potentially infectious materials. In situations where differentiation between body fluid types is difficult or impossible (i.e., uncontrolled or emergency situations), all body fluids shall be considered potentially infectious.

Additional information is available in the Environmental Safety Office or the Human Resources Office.

POLICY STATEMENTS REGARDING STATE AND FEDERAL STATUTES

IMMIGRATION REFORM AND CONTROL ACT

The Immigration Reform and Control Act (IRCA) of 1986 requires employers to ensure that each individual employed in any regular or temporary, full or part-time position is eligible to work in the United States. Certain procedures have been established to enable the University to comply with the provisions of this law. Failure to comply may result in fines and/or imprisonment.

The University's intent is to hire only authorized workers-- those who are eligible to work in the United States. All newly hired employees must provide government required proof of identity and authorization to work. Offers of employment must include a statement that employment is contingent upon proof of identity and authorization to work.

Each newly hired faculty member, executive/administrative/professional staff, support staff, graduate assistants/fellows and student employees are required to complete an Employment Eligibility Verification Form (Form I-9) on their first day of work.

Acceptable forms of identity include, but are not limited to, driver's license with photograph or an identification card issued by a state agency which includes a photograph. Proof of work authorization includes a Social Security card or a U.S. birth certificate. Documents which establish both identity and authorization to work include a passport, certification of citizenship or naturalization, a Resident Alien Card containing a photograph, or a non-U.S. passport bearing an endorsement of permission to work.

Questions pertaining to guidelines and procedures should be

directed to the Human Resources Office.

FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT

It is the policy of Indiana State University that all practices and procedures related to the education records of students will be in accord with the provisions of the Family Educational Rights and Privacy Act (FERPA) of 1974, as amended. This policy has been implemented by the development of guidelines and a listing of the education records on campus. Both the guidelines and the listing are available for review and copying through the University Legal Affairs Office.

EQUAL OPPORTUNITY / AFFIRMATIVE ACTION EMPLOYER

Equal Opportunity / Nondiscrimination Policy

Indiana State University has long been pledged to the principles of nondiscrimination and is firmly and unequivocally committed to the creation of a culturally diverse community among and between its faculty, staff, and students. Diversity within the University community advances the academic purpose of the University, and a nondiscrimination policy is essential to achieving such diversity. The University subscribes fully to all federal and state laws and regulations regarding discrimination.

Indiana State University does not discriminate on the basis of sex, race, age, national origin, sexual orientation, religion, disability, or veteran status. In line with its commitment to equal opportunity, the University will recruit, hire, promote,

educate, and provide services to persons based upon their individual qualifications meeting established criteria.

The University is committed to equal opportunity for employees and students through active recruitment, promotion, retention, and enrollment of individuals from the full spectrum of diverse populations, including people of color, women, persons with disabilities, and Vietnam-era veterans.

Responsibility for implementing the educational and employment decisions in accordance with the University's equal opportunity and nondiscrimination policy rests with the vice presidents, deans, directors, other heads of units, faculty, and staff. The Office of Diversity and Affirmative Action is responsible for overall compliance with all federal and state laws and regulations regarding nondiscrimination and for coordination of the University's commitment to education about, and celebration of campus diversity and international reach.

Furthermore, Indiana State University will not tolerate any form of sexual or racial harassment, intimidation, or coercion. Allegations of any form of harassment will be promptly and thoroughly investigated, and offenders will be subject to disciplinary action. The assistance and cooperation of the entire campus community are essential to transforming these words into demonstrated equal opportunity in academic programs and employment. (Equal Opportunity/Nondiscrimination Policy revised and approved by the Indiana State University Board of Trustees on October 24, 2003.) The Equal Opportunity/Affirmative Action Policy is presented in Appendix H.

DRUG-FREE WORKPLACE POLICY

The Drug-Free Workplace Act of 1988 required the adoption of a policy to create and maintain a drug-free workplace. Drug abuse in the workplace is contrary to the goals and objectives of Indiana State University. The policy of the University shall be as follows:

1. The unlawful manufacture, distribution, dispensation, possession, or use of controlled substances in any part of the University is prohibited.
2. The above is a condition of employment, and all employees must abide by its terms.
3. Any violation of this policy may be cause for:
 - a. Referral to the Employee Assistance Program for evaluation and assessment for possible treatment;
 - b. Participation in a drug rehabilitation program;
 - c. Suspension from duty; and/or
 - d. Termination of employment.
4. Programs will be available through the Employee Assistance Program to evaluate and inform employees about:
 - a. University policies pertaining to a drug-free workplace;
 - b. The dangers of drug abuse; and
 - c. The services and assistance provided confidentially by the Employee Assistance Program.
5. Any faculty or staff member convicted of a drug statute violation arising out of conduct occurring in the workplace must notify either the Human Resources Office or the appropriate vice president of the conviction no later than five (5) days after the conviction.

Failure to adhere to this policy can result in the University's ineligibility to receive any grant funds or federal contracts for up to five (5) years.

Further detailed information is available in the Human Resources Office.

DRUG-FREE SCHOOLS AND COMMUNITIES ACT AMENDMENTS OF 1989

The Higher Education Act of 1965, as amended by the Drug-Free Schools and Communities Act Amendments of 1989, requires that each institution of higher education receiving federal funds implement a drug prevention program on its campus and certify its compliance with the law to the Secretary of Education. The act requires clear delineation of standards of conduct for employees and students, educational programs and materials which are to be available to them, and sanctions which will apply for failure to meet expectations.

Indiana State University policy prohibits the unlawful manufacture, distribution, dispensation, possession, or use of controlled substances or alcohol in any part of the University or at any University activity. Legal use of alcohol may be permitted on campus only if approved by the University President or designee.

Any employee or student who is in violation of University policy or is convicted of a drug statute violation arising out of

conduct occurring in the workplace or at a University activity will be subject to any one or a combination of the following:

1. A verbal warning;
2. A written warning;
3. Disciplinary probation (students);
4. Referral to the Employee Assistance Program for evaluation, assessment, and counseling for possible treatment (employees);
5. Required participation in a drug or alcohol rehabilitation program;
6. Suspension from duty and/or enrollment; and/or
7. Termination of employment under standard University procedures.

Any employee or student referred for treatment or other rehabilitation will be required to complete the prescribed treatment as a condition of continued employment or enrollment.

Further information concerning legal sanctions under state and federal law may be secured from the University Legal Affairs Office.

FIREARMS AND OTHER DANGEROUS INSTRUMENTS

The ISU Board of Trustees is charged by statutes of the State of Indiana to govern the "use of the property owned, used or occupied by the institution, including the governance of travel over and assembly on such property" and the "conduct of students, faculty, staff or others while upon the property owned by or used or occupied by the institution". The Board is required "to protect the academic community from unlawful conduct or conduct which presents a serious threat to person or property of the academic community".

In furtherance of this responsibility, the transfer, use, or possession of explosives, fireworks, firearms, dangerous chemicals, or any lethal weapon on University property or in any fraternity or sorority house under circumstances except as part of a University authorized activity, instructional session, event, or duty is prohibited.

Pursuant to Indiana Code 20-12-3.V-1 and 20-12-3.V-2, the Indiana State University police officers are authorized to possess

and use firearms under such procedures as are currently in force or may hereafter be amended.

POLICY REGARDING SMOKING

Indiana State University has a commitment to the health and wellness of its students, faculty, and staff. This commitment is demonstrated by the Student Health Promotion and LeClub programs, by the efforts of the Employee Assistance Program, and by curricula and activities in several academic units throughout the University.

Documented research has substantiated the health problems caused by both smoking and passive smoke. The General Assembly of the State of Indiana adopted the Indiana Clean Indoor Air Law which is applicable to all state entities in order to address concern for the health and wellness of all Indiana government employees and students. This law sets forth minimum standards but allows state agencies to adopt more stringent rules if desired.

Indiana State University has established the following policy regarding smoking for all facilities and vehicles in which University functions or services are carried out or offered.

The sale of tobacco products is prohibited on university-owned, operated, or leased property.

The use of smoking tobacco products is prohibited on university-owned, operated, or leased property.

The use of smoking tobacco products is permitted in privately owned vehicles and in designated smoking areas on campus.

Any exceptions for the use of smoking tobacco products on university-owned, operated, or leased property must be approved by the President or Provost.

Enforcement of this policy will depend on the cooperation of all faculty, staff, and students not only to comply with the policy, but also to encourage others to comply, in order to promote a healthy environment in which to work study and live.

Observation of violation of the policy should be reported to Public Safety at 5555. Follow up for violations of the policy should be referred to the appropriate administrative office for review and action for faculty through the office of Academic Affairs, for staff through Human Resources and to the Dean of Students for students.

From spring through fall 2009, smoking cessation programs will be available to all employees and students at little or no cost to participants.

OPEN DOOR/OPEN RECORDS LAWS

It is the policy of Indiana State University to comply with the prescribed stipulations and the intent of legislation enacted by the Indiana General Assembly to make University meetings and records open to the public.

Open Door Law

The open door law requires that the governing body of any public agency and all public universities meet and conduct business in officially announced and open-to-the-public sessions. In addition, any committee of either an ad hoc or standing nature appointed directly by the governing body must conduct its meeting according to the same rules that inform meetings of the governing body. The intent of the statute is to ensure that decisions affecting the public and the public's interests are made in a public forum. The statute authorizes public observation. It does not authorize public participation.

The Indiana General Assembly clearly designed the statute to except from the open meeting requirement administrative, faculty, and student committees which are not appointed directly by the ISU Board of Trustees. However, the practice of Indiana State University is to conduct meetings of these administrative, student, and faculty committees in open session even though statute has no such requirement. Only administrative and academic committees which address personnel matters are closed to the press and the public. All other standing and ad hoc committees of the institution will conduct open meetings.

The University reserves the right, however, to apply its legislatively authorized and legal authority to close meetings of committees not appointed by the governing body. Meetings may be closed when a committee decides that the subject or nature of its deliberation is best served by meeting in closed session. The right to conduct a meeting closed to the public may also be exercised if the committee determines that an atmosphere of free and open discussion is jeopardized by an individual or group intent on the disruption of orderly processes. The chairperson of the committee, with the concurrence of a majority of the committee members, has the authority to close a meeting.

Should the committee be unable to agree or should anyone demand impediment toward the start or continuation of a meeting, the issue will be referred as soon as possible to the University Legal Affairs Office for review and decision. During the period of review, the activity of the committee will be suspended. When a meeting is closed without appropriate justification in the opinion of University legal counsel or the University President, the committee will be directed to conduct its business in public session.

Open (Access to Public) Records Law

The open records law of the State of Indiana requires that the public be afforded a right of access to public records. That right includes the inspection and copying of documents and records of state agencies and of public universities, so long as the request is made with reasonable particularity. The legislation does not authorize a general examination or exploration of the files of any agency of the State, nor does it require the state agency to compose documents which do not already exist.

In enacting the statute, the General Assembly has specifically excepted certain kinds of documents and records. Such documents include all records which may be classified by state or federal law or public agency or Supreme Court rules as confidential, those which are considered trade secrets or contain personal financial information, and those which are the instruments and results of research conducted under the auspices of the University, grade transcripts, license examinations, and patient medical records. Documents of like nature are confidential and are, therefore, not subject to the Indiana law on open records.

There are additional categories of records which Indiana law excepts, and the exercise of the exceptions is at the discretion of the public agency. Exceptions include, but are not limited to, law enforcement investigation records, certain kinds of legal work, test questions and their results, most personnel records, computer programs, codes, filing systems and software, records that are intra-agency or inter-agency advisory or deliberative material which contain opinions or information designed to serve as the basis for decision-making, diaries, journals or other personal notes, donor records, and library records. The statute is not designed or meant to make every document or record of the University on any and every subject available at any time to any person who makes a request.

Each request to review a University document or record presented under the prescribed stipulations and conditions of the public records law will be evaluated on its own merits. To facilitate the evaluation, the University will officially receive and respond to requests for review of or access to public records only in the Public Affairs Office for requests for information from the media, and in the University Legal Affairs Office for all other requests. All administrative or academic offices of the University will be instructed to refer all communications and requests to the appropriate office.

Under most conditions and circumstances, and in the majority of cases, documents and records will be made available upon request. Only in those instances in which the University is legally bound to maintain the confidentiality of records or in which it is authorized by law to make an exception will the University deny a request for access or review of a document or record. The exception and the grounds on which the exception

is made will be expressed by the Public Affairs Office or the University Legal Affairs Office, as appropriate.