November 14, 2019

ACTION: **Approve Information Security Program and First and Final Round Approval of New Board Policy 7003; Information Security Program and Revisions to Board Policy 5008; Employee Use of System Computers; Revisions to Board Policy 7004; Federal Personal Information Security Programs; Revisions to Board Policy 8064; Capital Construction and Information Technology (IT); Bids**

The System Office, Chadron State, Peru State, and Wayne State Colleges request approval of a newly developed system-wide Information Security Program (ISP). The NSCS ISP consists of a comprehensive set of cyber security policies and standards that will encourage standardization in IT practices and procedures across all three Colleges. New Board Policy 7003 establishes the NSCS ISP, and includes the creation sixteen cyber Standards. In addition, revisions to existing Board Policies 5008, 7004, and 8064, are necessary to bring them up to date with the new NSCS ISP.

In 2018, the three State Colleges and the System Office, with assistance from a cyber-security consultant, completed a risk assessment of NSCS IT systems. The top recommendation of the risk assessment was to develop a set of comprehensive, system-wide NSCS IT security policies to drive standardization and reduce the level of effort required to create and maintain documentation. Not only does a set of IT policies and standards guide the NSCS toward safer and more secure IT systems and practices, but it also assists with eventually meeting the requirements of the Gramm-Leach-Bliley Act (GLBA), a Federal law that applies to post-secondary institutions.

The System Office recommends approval of the Information Security Program; Board Policy 7003 & Revisions to Board Policies 5008, 7004 and 8064.

ATTACHMENTS:

- Board Policy 7003 (PDF)
- Revisions to Board Policy 5008 (PDF)
- Revisions to Board Policy 7004 (PDF)
- Revisions to Board Policy 8064 (PDF)
- ISP - Standards (PDF)

BOARD POLICY

Information Security Program (ISP)

The Board recognizes the importance of information security. The following shall constitute Board policy concerning information security.

Each College and the System Office will have an Information Security Program (ISP) which ensures availability, confidentiality and integrity of NSCS Technology Resources. Collectively, these programs will constitute the Information Security Program (ISP) for the NSCS, and this NSCS ISP shall satisfy the Gramm-Leach-Bliley Act (GLBA) requirements for non-public financial data.

The ISP will comply and align with other NSCS policies and shall be based on the Information Security Standards identified in this Policy.

Each President shall designate an individual responsible for each College ISP. The Vice Chancellor for Facilities and Information Technology shall be the individual responsible for the System Office ISP and shall serve as the System Office Information Security Officer (SOISO).

The SOISO shall coordinate with each President's designee to review the NSCS ISP no less frequently than annually, and to update as necessary.

To protect all Technology Resources of the NSCS, this Policy and NSCS ISP applies to all faculty, staff, students, visitors, vendors and contractors, and to all systems that access, store or transmit NSCS data.

In all Standards, the principles of least privilege, least functionality, and defense in depth, shall be applied.

Information Security Program Standards

Each College and the System Office shall implement and apply the following NSCS ISP Standards:

Standard 1: Definitions and Related Law, Policy and References
Standard 2: Responsibilities, Enforcement and Exceptions
Standard 3: Security Training and Awareness
Standard 4: Information Protection
Standard 5: Acceptable Use Policy
Standard 6: Computer and Network Security
Standard 7: Configuration and Change Management
Standard 8: Email
Standard 9: Physical Security
Standard 10: Technology Resources Acquisition
Standard 11: Payment Card Data Protection
Standard 12: HIPAA Security Rules and the HITECH Act
Standard 13: Cloud Computing
Standard 14: Information Systems Security Risk Management
Standard 15: Bring Your Own Device (BYOD)
Standard 16: Incident Management

Policy Adopted:

~~The Board of Trustees encourages employee use of computing and telecommunications technology in the performance of job duties in the System, especially in those areas involving teaching, instruction, research and public service.~~Board Policy 5008 references Board Policy 7003; NSCS Information Security Program, including the Security Standards defined by Board Policy 7003. Term definitions in Board Policy 5008 may be found in Standard 1, located here (URL-TBD).

~~Computing~~ Technology ~~r~~Resources~~, facilities and contracted services~~ provided by the Colleges and the System Office are the property of the Nebraska State College~~s~~ System (NSCS) and are to be used for the sharing of knowledge, ~~the creative process, and~~ collaborative efforts, and completion of job duties within the ~~Colleges'~~ NSCS educational, research and public service missions.

The NSCS reserves the right to inspect any NSCS Technology Resource without advance notice to or specific permission from any employee, for any legitimate business purpose.

The requirements in this ~~p~~Policy are to be followed by all ~~users of all~~employees utilizing State College Networks~~.~~

~~The provisions expressed in this policy also apply to~~ including all use~~rs~~ of any other networks that are accessed through an NSCS connection. Employees must comply with the NSCS Acceptable Use Policy (AUP) prior to gaining access to NSCS Technology Resources. The NSCS AUP is located in Standard 5, which may be found here (URL-TBD). The requirements found therein apply to all persons accessing or using NSCS Technology Resources, including NSCS students, employees, and authorized contractors and guests. Individuals that violate the NSCS AUP may be subject to denial of access and disciplinary action.

Acceptance of any credentials (i.e. username/password, ID card or token, PIN, etc.) that provide~~s~~ access to ~~computing~~ NSCS Technology ~~r~~Resources~~, facilities, contracted services and/or to NSCS information systems~~ shall constitute an agreement on behalf of the user or any other individual accessing such information to abide and be bound by the provisions of this ~~p~~Policy and the NSCS AUP. Access to NSCS ~~information systems~~ Technology Resources is a privilege, not a right. Every user is to be responsible for the integrity of the system, respect for the rights of other users, the integrity of the physical facilities and controls, and all pertinent license and contractual agreements related to ~~the college~~NSCS systems.

Employees shall make reasonable efforts to safeguard their credentials. No employee may allow unauthorized persons to access ~~to~~ College or System ~~data, computing or network~~Technology ~~r~~Resources, ~~facilities, and contracted services by sharing their credentials,~~ except in cases necessary to facilitate computer maintenance and repairs. When any employee terminates his or her employment ~~relationship or employment~~ with the College or System Office, his or her credentials shall be denied further access to ~~computing~~ Technology ~~r~~Resources~~, facilities, and contracted services~~ unless otherwise determined by the ~~College p~~President or Chancellor.

~~The Colleges and System Office are to make reasonable efforts to safeguard their computing resources, facilities, and contracted services through continuous improvement of both privacy and security of personal and institutional information and networks by implementing effective security practices and by creating a climate in which all users accept responsibility for protecting computing and information systems.~~

~~The use of electronic media and software provided for employee use by the Nebraska State College System are to be used for College or System related purposes.~~ Use of ~~computers, software, or other College or System equipment~~ Technology Resources for personal or commercial financial gain, for private business or commercial use, or for personal political or lobbying activities ~~is~~ are prohibited.

~~Use of College or System information systems, including computing resources, facilities, and contracted services is to be for college-related purposes.~~ Limited personal use of College or System ~~information systems~~ Technology Resources is permitted so long as such usage conforms with ~~p~~Policy, does not interfere with operations including, but not limited to, security of the system, network response time, or a user's performance of duties as an employee, and does not result in additional costs or inefficiencies to the College or System.

All users of College or System ~~electronic equipment and facilities~~Technology Resources are expected to respect the privacy of other users and their data in accordance to the NSCS AUP, and to respect the legal protection of programs, publications and data provided by copyright and licensing laws ~~to programs and data~~. All relevant laws and regulations, including public records laws, federal copyright laws, and federal privacy laws such as the Family Educational Rights to Privacy Act (FERPA) are to be respected by users. Downloading, distributing and/or displaying any copyrighted material without permission of the copyright owner is strictly prohibited.

~~To maintain the network, College or System technical personnel will routinely delete malware and other destructive and unrequested intrusions into information systems (viruses, spyware, etc.,) as they are detected.~~

~~Refusal to comply with these provisions and any other Federal, State or local laws that govern any aspects of computer and telecommunications use may result in denial of access to College or System Office information systems or other disciplinary action including suspension or termination of employment. The College or System Office may restrict or prohibit the use of its information systems in response to complaints presenting evidence of violations of College or System Office policies or state or Federal laws.~~

~~Users~~Consistent with the NSCS AUP, employees are also expected to respect the integrity of ~~computing systems~~Technology Resources and shall not intentionally execute programs that harass other users or infiltrate ~~a computer or computing~~ systems and/or damage or alter data ~~or the software components of a computer or computing system~~.

~~To prevent software viruses from infecting College or System Office computers and associated networks and to ensure network integrity and security, and to minimize unnecessary support incidents, it is the policy of the Board that only hardware and software approved in accordance with College or System Office procedures is to be installed on College or System Office computers. An employee with College or System Office provided computer training, which shall be available on a regular basis, and who can demonstrate a need to load such hardware or software is required to make advanced written request to the computing center or appropriate person designated by the College or System Office, produce proof of license for any software wishing to be installed, and to seek approval from the College or System Office, as appropriate, prior to the loading of such hardware or software.~~ To preserve the integrity and security of NSCS Technology Resources, NSCS employees purchasing information technology products and services must first consult with the College CIO, or the System Office. Refer to Board Policy 8064, and to Standard 10: Technology Resources Acquisition, in Board Policy 7003.

~~The College or System Office, as appropriate, reserves the right to inspect all electronic files, e-mail or voice mail of any employee, without advance notice or specific permission, for any legitimate business purpose.~~

~~Persons creating a web page are responsible for the accuracy of the information contained in the web page. Content should be reviewed periodically to assure continued accuracy. Web pages may include a phone number or email address of the person to whom questions/comments may be addressed, as well as the most recent revision date.~~

Each College, affiliate organization, and the System Office is responsible for employee use of ~~computing and telecommunications t~~Technology Resources and for ensuring that its ~~users~~employees are familiar with the provisions outlined in this ~~p~~Policy and in the NSCS AUP.

Policy Adopted: 11/11/95
Policy Revised: 2/10/05
Policy Revised: 4/25/14
Policy Revised:

POLICY: 7004 Federal Personal Information Security Programs

BOARD POLICY

Identity Theft Prevention Program

The Board recognizes the importance of identity theft prevention. The Board also recognizes that the Colleges currently maintain certain "covered accounts" as defined by the Federal Trade Commission (FTC) that include loan programs and payment plans. In response to the FTC's issuance of "Red Flag Rules", each College will establish and maintain an Identity Theft Prevention Program that includes identification, detection, prevention and mitigation of identity theft risks. The programs should be periodically reviewed and updated to consider changes to the plan in response to the changing environment.

A Red Flag, as included in the FTC's rules, and also included below, is defined as a relevant indicator of a possible risk of identity theft. The Identity Theft Program should include, at a minimum, the following sections:

1) Identification
In identifying Red Flags, each College should consider the types of covered accounts it offers and maintains, the methods it provides to open and access its covered accounts, and its previous experiences with identity theft.

2) Detection and Prevention
Each program should include consideration of the detection of Red Flags in connection with the covered accounts. The program should also include obtaining identifying information about, and verifying the identity of, a person opening a covered account. This information should then be used to authenticate customers, monitor transactions, and verify the validity of change of address requests.

3) Response
Each program should provide for appropriate responses to detected Red Flags to prevent and mitigate identity theft.

Each program should be reviewed and updated periodically to reflect changes in risks such as:
*experiences with identity theft
*changes in methods of identity theft
*changes in methods to detect, prevent, and mitigate identity theft
*changes in service provider arrangements

Each College shall submit its initial Identity Theft Program for approval by the Board. Thereafter, a copy of each College's current program and annual report on compliance shall be kept on file at each College. Each College President, or designee, will be responsible for oversight of the Identity Theft Program at their ~~e~~College.

~~**Customer Information Security Program**~~

~~The Board recognizes the importance of protecting non public student financial information. The Board further recognizes that by virtue of the Colleges' participation in the Title IV Federal student financial aid programs authorized under Title IV of the Higher Education Act, each College is subject to certain requirements of the Gramm Leach Bliley Act (GLBA).~~

~~The Board directs each College to develop an Information Security Program to protect non public financial information consistent with the following policy.~~

~~Each College must identify and periodically assess external and internal risks to the security, confidentiality, and integrity of non-public financial information. These risks may include:~~

- ~~Unauthorized access to information by individuals other than employees with a legitimate purpose for viewing such information;~~
- ~~Breaches of computer network security resulting in unauthorized access or transfer of information to third parties;~~
- ~~Physical loss of data resulting from fire, flood or other disaster;~~
- ~~Unauthorized requests and releases of information to third parties; and~~
- ~~Unauthorized access through hardcopy files or reports.~~

~~Each College must establish a written plan and procedures to manage and control the risks. The plan and procedures must specifically address information gathered and maintained through College computer systems and in all physical files. Additionally, the plan must provide for the training of employees regarding the importance of confidentiality of student records, student financial information, and other types of non public data and information. The plan and procedures shall be periodically reviewed and updated in order to address changes in risks, technology or the sensitivity of the information.~~

~~Each College President shall designate an individual responsible for the development, implementation, and periodic review of the plan and procedures. Each College must submit its written plan and procedures to the System Office and maintain a current copy on file along with a record of the periodic reviews of the plan and procedures.~~

Policy Adopted: 1/13/09
Policy Revised: 3/24/17
Policy Revised:

BOARD POLICY

Applicability

Board Policy 7010 applies to bidding and purchases of general items, supplies and ordinary services. Board Policy 7016 applies to contracts for legal counsel, auditor, lobbyists, search consultants, and other consultants and specialized services not associated with facilities or information technology in the 8000 series Board policies. Policy 8064 applies to construction, facilities and Information Technology (IT) related purchases and bidding, and includes facilities related purchases such as carpet/flooring & wall finishes, equipment, fixtures, furnishings, and window coverings even when their purchase is not associated with a capital construction project. The following four sections: **Emergency**; **Sole Source**; **Exceptions to Bidding Requirements**; and **Requests for Proposals (RFP)**, apply to both Board policies 7010 and 8064.

Emergency

Emergency shall mean any situation where it is necessary to enter into a contract to (a) avoid the loss of life, health, safety, or property, (b) respond to time limits established by an external authority, (c) ensure the continuation of an essential College service, function, utility, facility or ~~computer/software system~~Technology Resource, or (d) avoid, correct or repair a situation outside the control of the Colleges including detrimental negligence or acts of an employee, natural or manmade disasters, and security or data compromise.

Proposed emergency purchases shall be documented by the College unit or department, and submitted to the Vice President for Administration and Finance, for approval by the Chancellor. The Chancellor may also approve the suspension of bidding requirements as appropriate for each emergency.

Sole Source

A sole source purchase is when there is only a single feasible or sole source for the supplies or services. A single feasible or sole source exists when:

- Supplies are proprietary and only available from the manufacturer or a single distributor.
- Additions to a system must be compatible with the original equipment or software.
- Factory authorized maintenance must be utilized in order to maintain validity of a warranty.
- Only one (1) type of computer software exists for a specific application.
- The software or materials are copyrighted and are only available from the publisher or a single distributor.
- The services of a particular provider are unique, e.g. entertainers, authors, etc.
- Based on current research, it is determined that only a single distributor services the region in which the supplies are needed.

Documentation to purchase based on sole source without competitive bids or proposals shall be documented by the College unit or department, and approved by the Vice President for Administration and Finance in consultation with either the Vice Chancellor for Facilities and Information Technology, or the Vice Chancellor for Finance and Administration.

Exceptions to the Bidding Process

Exceptions to the bidding process are defined as: emergency and sole source purchases with proper approval, advertising, software licensing renewals and software/hardware maintenance agreements, purchase from a previously competitively bid government or multi-state compact contract, including other state colleges and higher education institutions, or when the price has been established by the federal General Services Administration. Exceptions also include repairs of less than fifty thousand dollars ($50,000) for vehicles, equipment, furnishings, Information Technology hardware/software/systems, and facilities/grounds. Repairs under $50,000 require negotiation to assure quality work is performed at a reasonable price.

Requests for Proposals (RFP)

A Request for Proposal (RFP) process includes a detailed description of the items/supplies/services/systems desired, but important factors other than cost are made part of the process and considered in the award of the contract. For the purpose of Board policies, an RFP can be considered a form of bidding, and may be used when formal or informal bidding is required. The exception to that is when a proposal is received through an RFP process for the purpose of selecting a design/construction consultant or contractor in Board policies 8066 and 8071. In such cases, the proposals are not considered "bids" since the final contract amount is derived through negotiations with the highest ranked firm.

The Board shall, within the limits prescribed by law, prepare specifications, advertise projects, evaluate and award all bids for capital construction projects and information technology related purchases in the System.

No College employee or Board member shall furnish or cause to be furnished any technical information, or solicit proposals and/or prices or take any type of action, which would or could be construed to give a direct or indirect advantage or disadvantage to a potential bidder for a College Project.

No person shall attempt to influence in any way or participate or assume responsibility in the evaluation of proposals and selection of contractors when participation constitutes a conflict of interest.

FORMAL PROCEDURE

Construction projects and information technology related purchases exceeding one hundred thousand dollars ($100,000) shall observe the following bidding procedures:

1. Specifications: All specifications and plans for buildings to be renovated or constructed, are to be prepared by professional architects and/or engineers when required by state law. The specifications and plans shall be prepared in such a manner that the completed building, landscaping and parking facilities, including the cost of equipment and fixtures necessary for the project, or the completed renovation cost shall not exceed the amount authorized for that purpose. Specifications for information technology related purchases may be prepared by College ~~employed technicians~~information technology staff or hired consultants.

2. Advertising project: For construction, the public notice shall appear once a week for three (3) consecutive weeks in a publication based in or near the locality of the project and in other widely circulated publications as deemed necessary by the College. The notice shall not appear on a weekend or holiday. A minimum of fifteen (15) calendar days shall elapse between the time formal bids are first advertised or called for and the time of their opening. For information technology procurement, the College determines the most effective means of advertising and distributing the Request for Proposals (RFP).

The notice or RFP shall include, at a minimum, the following information:

a) Name of Board of Trustees/College
b) Description of project
c) Date, place and time when bids must be received
d) Person to contact for information
e) Locations where bid documents can be viewed/obtained

A copy of the advertisement shall be kept on file with the College responsible for placing the advertisement and will be made available to the System Office upon request.

3. Bid Opening for Construction: Bids shall be submitted in a sealed envelope with notation of the project on the front. Bids shall be opened on the date, time and place as advertised. The bid opening shall be conducted in public so that all bidders and interested parties may be present. No bids are to be received after the specified time and are to be returned unopened. The bidder's envelope is to be attached to the back of the bid form. The professional consultant shall be responsible for opening and reading aloud the bids. Bid documents shall be considered public information after they have been opened. The following requirements shall be noted at the time of opening the bid:

a) Conformance with bidding instructions
b) Use of proper bid forms
c) Accompanied by bid bond or certified check (not applicable to information technology)
d) Acknowledgment of any addendum
e) Bid is signed

For information technology RFP's, proposal submissions generally follow the bid opening procedures above, except that electronic proposals may be accepted.

4. Bid Evaluation for Construction: When bids are received, publicly opened and read, the contractors shall not be notified of the final decision until a later date so that adequate study and analysis can be made of the bids received. The professional consultant shall evaluate the bids received and make a recommendation to the College. Awarding of the contracts shall be based on competitive bidding with award to the lowest responsible bidder, taking into consideration the best interests of the State of Nebraska and the System, the quality or performance of the firm and the materials to be supplied, their conformity with specifications, and the times of completion. In determining the lowest responsible bidder, in addition to price, the following elements shall be given consideration:

a) The ability, capacity, and skill of the bidder to perform the contract required;
b) The character, integrity, reputation, judgment, experience, and efficiency of the bidder;
c) Whether the bidder can perform the contract within the time specified;
d) The quality of performance of previous contracts;
e) The previous and existing compliance by the bidder with laws relating to the contract;
f) The life-cost of the article or property in relation to the purchase price and the specific use of the item;
g) The performance of the article or property, taking into consideration any commonly accepted tests and standards of product usability and user requirements;
h) Energy efficiency ratio as stated by the bidder for alternative choices of appliances or equipment; and
i) Such other information as may be secured having a bearing on the decision to award the contract.

For information technology RFP's, proposal evaluation generally follows the construction bid evaluation procedures above, except that the contract is not necessarily awarded to the lowest cost proposal, but to the top ranked proposal based on the criteria outlined in the RFP.

When a public contract is to be awarded to the lowest responsible bidder, a resident bidder shall be allowed a preference over a nonresident bidder from a state which gives or requires a preference to bidders from that state.

A capital construction or information technology contract may be conditioned upon later refinements in scope and price and may permit the College in agreement with the contractor to make changes in the project without invalidating the contract. Later refinements shall not exceed the scope of the program statement or available funding.

All bidders on College projects must file a statement that they are complying with, and will continue to comply with, fair labor standards in the pursuit of their business and in the execution of the contract on which they are bidding. All bidders must also comply with the State of Nebraska's Drug-Free Workplace requirement. The proposal form used to bid projects shall contain a clause which, when the proposal is signed by the bidder, certifies that the firm has a drug-free workplace policy in accordance with State requirements.

The contractor must specifically agree not to discriminate against any recipient of services on the basis of race, color, sex, religion, creed, age, marital status, physical or mental disability, political affiliation, national origin or ancestry, and not to discriminate against any employees or applicant for employment on the basis of race, color, sex, religion, creed, age, marital status, physical or mental disability, political affiliation, national origin or ancestry.

All contracts will contain equal opportunity statements to ensure compliance with Federal Government requirements associated with Title VI and Title VII of the Civil Rights Act of 1964, and other appropriate equal opportunity procurement policies.

The recommendation, bid tab sheet and other applicable materials shall be provided to the System Office for review. In the event that less than three (3) bids or proposals are received, the Vice Chancellor for Facilities and Information Technology may approve award of contract based on documentation received. Approval of less than three (3) bids only applies to the Formal Procedure.

For any construction project that has a total cost of more than one hundred thousand dollars ($100,000), the successful bidder for the project shall be required to furnish a Performance Bond and a Labor Material Payment Bond, each in the amount of 100% of the contract sum, written by a Surety licensed to do business in the State of Nebraska.

If the recommendation is to reject the lowest bid for any one or more of the reasons stated above, the recommendation must include the reason(s) for the rejection. The Board always reserves the right to reject any or all bids.

INFORMAL PROCEDURE

Construction projects and information technology related purchases with a total project cost between thirty thousand dollars ($30,000) and one hundred thousand dollars ($100,000) shall observe the following bidding procedure:

1. Three or more quotations for the project shall be solicited from responsible bidders. Original quotations may be obtained in writing or verbally. Any verbal quotations must be followed up with a written or faxed confirmation for project files.

2. A fixed bid receipt date or public opening is not required.

3. A formal contract shall be executed for the project after negotiating a price that is reasonable and within budget. The contract may be the System's short form, long form, or other form acceptable to the Vice Chancellor for Facilities and Information Technology

   A capital construction or information technology purchase contract may be conditioned upon later refinements in scope and price and may permit the College in agreement with the contractor to make changes in the project without invalidating the contract. Later refinements shall not exceed the scope of the program statement or available funding.

4. All resulting quotations or refusals to quote shall be documented by the College for reference.

5. Information on these contracts shall be reported to the Board of Trustees at the first Board meeting following College acceptance of the contract.

OPEN SOLICITATION

Construction projects and information technology related purchases with a total cost of less than thirty thousand dollars ($30,000) shall follow the open solicitation process, as follows:

1. Competitive bidding is not required.

2. The College may contract directly with a responsible contractor after negotiating a contract price that is reasonable and within budget.

3. A capital construction or information technology purchase contract may be conditioned upon later refinements in scope and price and may permit the College in agreement with the contractor to make changes in the project without invalidating the contract. Later refinements shall not exceed the scope of the program statement or available funding.

INFORMATION TECHNOLOGY (IT) PURCHASING

Security of data, and ~~College IT systems infrastructure~~ requirements for NSCS ~~t~~Technology ~~r~~Resources ~~networks~~, need to be considered when ~~College departments or units~~NSCS employees make IT purchases. In accordance with Standard 10: Technology Resources Acquisition, from the NSCS Information Security Program in Board Policy 7003, ~~Purchases should be coordinated with the College IT department~~ all employees must consult with the applicable Chief Information Officer (CIO) or System Office Information Security Officer (SOISO) before developing, purchasing or contracting for products, services, and/or consulting that have implications for ~~t~~Technology ~~r~~Resource components, data, ~~or~~ security, or technical support. This includes, but is not limited to, cloud services, communication systems, information storage and processing systems, software systems, physical facilities related to such systems, and contractual relationships with vendors of such systems and services.~~when the purchases involve hardware or software to be installed on premise, consulting or professional service engagements which will require IT integration or services, and Cloud services which will, at any time during the contract, be used to store or handle data that is: 1) PII-Personally Identifiable Information beyond the scope of the user requesting the service, 2) FERPA protected, 3) requires Institutional Research Board (IRB) approval, or is 4) non-public institutional data.~~

Legal Reference:	RRS 72-802	Public buildings; plans and specifications; limitations; bids; appropriations; limits
	RRS 72-803	Public buildings; construction; improvement and repair; contracts; bidding; procedure; exceptions
	RRS 73-101.01	Public lettings; resident bidder; defined; preference
	RRS 73-102	Fair Labor Standards, statement of compliance required.
	RRS 81-1108.43	Capital construction project; prohibited acts; exceptions; warrant; when issues
	RRS 81-1114	Department of Administrative Services; building division; powers, duties, and responsibilities
	RRS 85-304	Board of Trustees; powers; enumerated
	RRS 81-3449	Practice of architecture; exempted activities
	RRS 81-3453	Practice of engineering; exempted activities

Policy Adopted:	3/11/94
Policy Revised:	8/29/97
Policy Revised:	10/29/97
Policy Revised:	9/10/02
Policy Revised:	2/12/04
Policy Revised:	9/15/06
Policy Revised:	9/14/07
Policy Revised:	9/11/09
Policy Revised:	4/22/10
Policy Revised:	6/2/11
Policy Revised:	6/18/15
Policy Revised:	11/17/17
Policy Revised:	6/18/19
Policy Revised:	