From: Office of the University Counsel and
Vice Chancellor for Legal Affairs
Office of the Vice Chancellor
for University Affairs and Development
Personal Privacy Protection Law

Subject: Office of the University Counsel and
Vice Chancellor for Legal Affairs
Office of the Vice Chancellor
for University Affairs and Development
Personal Privacy Protection Law

To: Presidents, State-operated Campuses

A new law, the "Personal Privacy Protection Law," which is designed to protect the privacy rights of individuals to whom state agency records pertain, becomes effective September 1, 1984. This law imposes a number of requirements on state agencies with respect to collection, maintenance, access to and disclosure of records containing personal information about individuals ("data subjects"). It is applicable to all state-operated campuses of the State University but does not apply to the community colleges. The Committee on Open Government, which has statewide responsibility to provide advice on implementation of the Freedom of Information Law and the Open Meetings Law, has been given similar responsibilities with respect to the Personal Privacy Protection Law. A copy of the law is attached for your information (Attachment A).

The following is a brief summary of the major requirements of the law:

A. Access to Personal Information

State agencies must allow access by data subjects to records containing personal information about them. With respect to the State University, such records include employee, student and alumni records. It is important to note that certain records, such as medical records and public safety agency records, are exempted from this accessibility requirement. You should also know that there are unresolved questions which we are attempting to clarify relating to employee access under this law to certain personnel records not accessible to employees under the various collective bargaining agreements.

Each agency must promulgate rules setting forth procedures by which a data subject can learn if any agency records pertain to him or her, obtain access to such records and amend or correct such records. In accordance
with this provision, on June 27, 1984, the Board of Trustees adopted regulations governing access to and correction or amendment of personal information maintained by the University and the campuses. The regulations, which are effective September 1, 1984, follow, in general, the format of the procedures established by the University to implement the Freedom of Information Law. A copy of the regulations (Part 315, Title 8, Official Compilation of Codes, Rules and Regulations of the State of New York) is enclosed as Attachment B.

The regulations require the chief administrative officer of each campus to designate a "privacy compliance officer" who shall be responsible for ensuring appropriate responses to requests for access to and for amendment and correction of records in accordance with the law. We recommend that you consider designating as the campus privacy compliance officer the individual who is serving as the campus records access officer under the University's Freedom of Information Law regulations. The designation should be made prior to September 1, 1984, the effective date of the regulations. We would appreciate it if you would advise Richard Gillman, Assistant Vice Chancellor for University Affairs, of the name of the individual designated as the campus privacy compliance officer so that we can provide that officer with additional information on this law.

B. Notices of Systems of Records

Each campus must prepare and submit to the Committee on Open Government Notices of Systems of Records within 30 business days of the law's effective date. "Systems of Records" are defined by the law as "...any group of records under the actual or constructive control of any agency pertaining to one or more data subjects from which personal information is retrievable by use of the name or other identifier of a data subject." (emphasis added). New systems of records developed after September 1, 1984 must be reviewed by the Committee on Open Government prior to their implementation.

Notices of systems of records have already been prepared by the State University at Buffalo and the State University Hospital of Upstate Medical Center which can be used by the campuses as models from which to develop their own notices. We will be pleased to share these notices with the campus privacy compliance officers.

C. Notification to Data Subjects

Every individual from whom a campus requests personal information which will be maintained in a record must be given notification at the time of the initial request of the purpose(s) for collecting the information, the legal authority for such collection, the use(s) which
will be made of the information and the name of the system of records in which the information will be maintained.

A sample notification form has been prepared by the Committee on Open Government which we will provide to the campus privacy compliance officers.

D. Disclosures to Third Parties

No record containing personal information may be disclosed to third parties without the consent of the data subject unless the disclosure is made to individuals or entities specified in the law or pursuant to a subpoena or other compulsory legal process.

In certain limited circumstances, an accounting of disclosures must be maintained as part of the data subject's file for five years or the life of the record whichever is larger. A sample accounting of disclosures form has been developed which includes instructions on when such accountings must be maintained.

E. Development and Maintenance of Systems of Records

Each campus is required to develop: (1) written policies regarding the responsibilities of persons involved in the development and operation of systems of records; (2) safeguards for the security of such systems and (3) rules governing retention and timely disposal of records. (The University already has rules governing retention and disposal schedules for its records which are set forth in the SUNY Records Retention and Disposition Manual.)

Our offices will be scheduling workshops in the early fall which will serve to familiarize privacy compliance officers and other appropriate campus administrators with the requirements of the Personal Privacy Protection Law. In the interim, questions concerning compliance with the law's requirements should be directed to Carolyn Pasley, Associate Counsel (518-473-7591) or Richard Gillman, Assistant Vice Chancellor for University Affairs (518-473-1825).

Robert Perrin
Sanford H. Levine

Copies for information only sent to:

Presidents, Community Colleges
Deans, Statutory Colleges
President Coll
Vice Provost Spencer
§91. Short title. This article shall be known as the “personal privacy protection law”.

§92. Definitions. (1) Agency. The term “agency” means any state board, bureau, committee, commission, council, department, public authority, public benefit corporation, division, office or any other governmental entity performing a governmental or proprietary function for the state of New York, except the judiciary or the state legislature or any unit of local government and shall not include Offices of district attorneys.

(2) Committee. The term “committee” means the committee on open government as constituted pursuant to subdivision one of section eighty-nine of this chapter.

(3) Data subject. The term “data subject” means any natural person about whom personal information has been collected by an agency.

(4) Disclose. The term “disclose” means to reveal, release, transfer, disseminate or otherwise communicate personal information or records orally, in writing or by electronic or any other means other than to the data subject.

(5) Governmental unit. The term “governmental unit” means any governmental entity performing a governmental or proprietary function for the federal government or for any state or any municipality thereof.

(6) Law. The term “law” means state or federal statute, rule or regulation.

(7) Personal information. The term “personal information” means any information concerning a data subject which, because of name, number, symbol, mark or other identifier, can be used to identify that data subject.

(8) Public safety agency record. The term “public safety agency record” means a record of the commission of corrections, the temporary state commission of investigation, the department of correctional services, the division for youth, the division of parole, the crime victims board, the division of probation or the division of state police or of any agency or component thereof whose primary function is the enforcement of civil or criminal statutes if such record contains information, law enforcement, confinement of persons in correctional facilities or supervision of persons pursuant to criminal conviction or court order, and any records maintained by the division of criminal justice services pursuant to sections eight hundred thirty-seven, eight hundred thirty-seven-a, eight hundred thirty-seven-b, eight hundred thirty-seven-c, eight hundred thirty-eight, eight hundred thirty-nine, eight hundred forty-five, and eight hundred forty-five-a of the executive law.

(9) Record. The term “record” means any item, collection or grouping of personal information about a data subject which is maintained and is retrievable by use of the name or other identifier of the data subject. The term “record” shall not include personal information which is not used to make any determination about the data subject if it is:

(a) a telephone book or directory which is used exclusively for telephone and directory information;

(b) any card catalog, book or other resource material in any library;

(c) any compilation of information containing names and addresses only which is used exclusively for the purpose of mailing agency information;

(d) personal information required by law to be maintained, and required by law to be used, only for statistical research or reporting purposes;

(e) information requested by the agency which is necessary for the agency to answer unsolicited requests by the data subject for information; or

(f) correspondence files.

(10) Routine use. The term “routine use” means, with respect to the disclosure of a record or personal information, any use of such record or personal information relevant to the purpose for which it was collected, and which is necessary to the statutory duties of the agency that collected or obtained the record or personal information, or necessary for that agency to operate a program specifically authorized by law.

(11) System of records. The term “system of records” means any group of records under the actual or constructive control of any agency pertaining to one or more data subjects from which personal information is retrievable by use of the name or other identifier of a data subject.

§93: Powers and duties of the committee. (1) The committee shall prepare a directory derived from the information provided pursuant to section three of chapter six hundred seventy-seven of the laws of nineteen hundred eighty and subdivision one of section ninety-four of this article. The directory shall include the name of each system of records subject to the provisions of this article, the name and subdivision of the agency maintaining it, the title and business address of the person responsible therefor, the approximate number of data subjects and the categories of information collected; and sufficient information for the identification of rules promulgated by agencies pursuant to this article. Individuals shall be permitted to purchase the directory for a reasonable price as set by the committee in accordance with law.

(2) The committee may, upon request of a data subject eligible therefor, make a request under section ninety-five of this article, investigate, make findings and furnish an advisory opinion in connection with the requirements of section ninety-five of this article. Prior to the issuance of an advisory opinion, the committee may require an agency to provide additional information which the committee deems necessary to render an opinion. However, no system of records exempt from the provisions of section ninety-five of this article shall be subject to the provisions of this subdivision.

(3) Within thirty business days of the receipt of a privacy impact statement or supplemental statement by an agency the committee shall review such statement to determine whether the maintenance of the system is within the lawful authority of the agency and to determine whether there have been established rules and procedures as required by section ninety-four of this article. However, such review by the committee shall not infringe upon or maintain by such agency. After review of such information the committee may notify the agency of the result of its review. Such notification and result shall not constitute an advisory opinion and shall not be reported as such by the committee and there shall be no obligation upon the agency to respond to such notification or result.

(4) The committee shall promulgate rules for the specification of the form of the privacy impact statement. Such privacy
§ 94. Agency obligations. (1) Each agency that maintains a system of records shall:

(a) except when a data subject provides an agency with unsolicited personal information, maintain in its records only such personal information which is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or executive order, or to implement a program specifically authorized by law;

(b) consistent with the standards of paragraph (a) of this subdivision, maintain all records used by the agency to make any determination about any data subject with accuracy, relevance, timeliness and completeness provided however, that personal information or records received by an agency from another governmental unit for inclusion in public safety agency records shall be presumed to be accurate;

(c) collect personal information directly from the data subject whenever practicable, except when collected for the purpose of making quasi judicial determinations;

(d) provide each data subject whom it requests to supply information to be maintained in a record, at the time of the initial request, with notification as provided in this paragraph. Where such notification has been provided, subsequent requests for information from the data subject to be maintained in the same record need not be accompanied by notification unless the initial notification is not applicable to the subsequent request.

§94. Agency obligations. (1) Each agency that maintains a system of records shall:

(a) except when a data subject provides an agency with unsolicited personal information, maintain in its records only such personal information which is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or executive order, or to implement a program specifically authorized by law;

(b) consistent with the standards of paragraph (a) of this subdivision, maintain all records used by the agency to make any determination about any data subject with accuracy, relevance, timeliness and completeness provided however, that personal information or records received by an agency from another governmental unit for inclusion in public safety agency records shall be presumed to be accurate;

(c) collect personal information directly from the data subject whenever practicable, except when collected for the purpose of making quasi judicial determinations;

(d) provide each data subject whom it requests to supply information to be maintained in a record, at the time of the initial request, with notification as provided in this paragraph. Where such notification has been provided, subsequent requests for information from the data subject to be maintained in the same record need not be accompanied by notification unless the initial notification is not applicable to the subsequent request.
(c) at the request of the data subject, inform any person or other governmental unit to which a disclosure has been or is made of any correction, amendment, or notification of dispute made by the agency, provided that an accounting of the prior disclosure was made or that the data subject to whom the record pertains provides the name of such person or governmental unit;

d) with respect to a disclosure made for inclusion in a public safety agency record or to a governmental unit or component thereof whose primary function is the enforcement of civil or criminal statutes, notify the receiving governmental unit that an accounting of such disclosure is being made pursuant to this subdivision and that such accounting will be accessible to the data subject upon his or her request unless otherwise specified by the receiving governmental unit pursuant to paragraph (e) of this subdivision;

(e) with respect to a disclosure made for inclusion in a public safety agency record or to a governmental unit or component thereof whose primary function is the enforcement of civil or criminal statutes, if in its request for the record the receiving governmental unit states that it has determined that access by the data subject to the accounting of such disclosure would impede criminal investigations and specifies the approximate date on which such determination will no longer be applicable, refuse the data subject access to such accounting or information that such accounting has been made, except upon court ordered subpoena, during the applicable time period. Upon the expiration of said time period the disclosing agency shall inquire of the receiving governmental unit as to the continued relevancy of the initial determination and, unless requested in writing by the receiving governmental unit to extend the determination for a specified period of time, shall make available to the data subject an accounting of said disclosure; and

(7) in making a disclosure pursuant to subdivision one of section ninety-six of this article, an agency shall make such disclosure pursuant to paragraph (d), (i) or (j) of said subdivision only when such disclosure cannot be made pursuant to any other paragraph of said subdivision.

(4) (a) Any agency which established or substantially modified a system of records after December fifteenth, nineteen seventy-seven of the laws of nineteen hundred eighty within thirty business days of the effective date of this article.

(b) Any agency which seeks to establish a system of records subsequent to the effective date of this article shall file with the committee a privacy impact statement as prescribed by subdivision four of section ninety-three of this article. Any agency which seeks to modify a system of records in a way which would render inaccurate any information set forth in the privacy impact statement, in the notice described in paragraph (a) of this subdivision or in the notice filed pursuant to chapter six hundred seventy-seven of the laws of nineteen hundred eighty, shall file notice with the committee pursuant to chapter six hundred seventy-seven of the laws of nineteen hundred eighty within thirty business days of the effective date of this article.

(b) Any agency which seeks to establish a system of records subsequent to the effective date of this article shall file with the committee a privacy impact statement as prescribed by subdivision four of section ninety-three of this article. Any agency which seeks to modify a system of records in a way which would render inaccurate any information set forth in the privacy impact statement, in the notice described in paragraph (a) of this subdivision or in the notice filed pursuant to chapter six hundred seventy-seven of the laws of nineteen hundred eighty, shall file with the committee a supplemental statement to conform the privacy impact statement or notice to the proposed modification. Unless the date by which such proposed system or modification is required by law to be instituted is less than thirty business days from the date of the filing of the privacy impact statement, no such proposed system or modification shall be instituted until the completion of the procedures set forth in subdivision three of section ninety-three of this article.

(5) Each agency shall, within fifteen business days of the receipt of an advisory opinion issued by the committee, respond in writing to the committee as to the following:

(a) the actions it has taken, or will take, to comply with the advisory opinion; or

(b) the reasons for disagreement and noncompliance with the advisory opinion.

(6) On or before the first day of September of each year, each agency shall submit a report covering the preceding year to the committee. The report shall include, with respect to requests for access to records and with respect to requests for correction or amendment of records pursuant to subdivisions one and two of section ninety-five of this article, respectively, the following information:

(i) the number of determinations made to grant such requests; and

(ii) the number of determinations made to deny such requests, in whole or in part, respectively.

(7) The provisions of paragraphs (c) and (d) of subdivision one of this section shall not apply to the following:

(a) personal information that is collected for inclusion in a public safety agency record;

(b) personal information that is maintained by a licensing or franchise-approving agency or component thereof for the purpose of determining whether administrative or criminal action should be taken to restrain or prosecute purported violations of law, or to grant, deny, suspend, or revoke a professional, vocational, or occupational license, certification or registration, or to deny or approve a franchise;

(c) personal information solicited from a data subject receiving services at a treatment facility, provided that each such data subject shall, as soon as practicable, be provided a notification including information specified in subparagraphs (l), (ii), (iii), (iv), (v) and (vi) of paragraph (d) of subdivision one of this section describing systems of records concerning the data subject maintained by the treatment facility.

(8) The provisions of subdivisions two, three and six of this section shall not apply to public safety agency records.

(9) Nothing in this article shall abrogate in any way any obligation regarding the maintenance of records otherwise imposed on an agency at law or in equity.
described, pertaining to that data subject, which he or she believes is not accurate, relevant, timely or complete, either:
(a) make the correction or amendment in whole or in part, and inform the data subject that upon his or her request such correction or amendment will be provided to any or all persons or governmental units to which the record or personal information has been or is disclosed, pursuant to paragraph (c) of subdivision three of section ninety-four of this article; or
(b) inform the data subject of its refusal to correct or amend the record and its reasons therefor.

(3) Any data subject whose request under subdivision one or two of this section is denied in whole or in part may, within thirty business days, appeal such denial in writing to the head, chief executive or governing body of the agency, or the person designated as the reviewing official by such head, chief executive or governing body. Such official shall within seven business days of the receipt of an appeal concerning denial of access, or within thirty business days of the receipt of an appeal concerning denial of correction or amendment, either provide access to or correction or amendment of the record sought and inform the data subject that, upon his or her request, such correction or amendment will be provided to any or all persons or governmental units to which the record or personal information has been or is disclosed, pursuant to paragraph (c) of subdivision three of section ninety-four of this article, or fully explain in writing to the data subject the factual and statutory reasons for further denial and inform the data subject of his or her right to thereupon seek judicial review of the agency’s determination under section ninety-seven of this article. Each agency shall immediately forward to the committee a copy of such appeal, the determination thereof and the reasons therefor.

(4) If correction or amendment of a record or personal information is denied in whole or in part upon appeal, the agency shall inform the data subject of the right to file with the agency a statement of reasonable length setting forth the reasons for disagreement with the agency’s determination and that, upon request, his or her statement of disagreement will be provided to any or all persons or governmental units to which the record has been or is disclosed, pursuant to paragraph (c) of subdivision three of section ninety-four of this article. With respect to any personal information about which a data subject has filed a statement of disagreement, the agency shall clearly note any portions of the record which are disputed, and shall attach the data subject’s statement of disagreement as part of the record. When providing the data subject’s statement of disagreement to other persons or governmental units pursuant to paragraph (c) of subdivision three of section ninety-four of this article, the agency may, if it deems appropriate, also include in the record a concise statement of the agency’s reasons for not making the requested amendment.

(5) (a) Any agency which may not otherwise exempt personal information from the operation of this section may do so, unless access by the data subject is otherwise authorized or required by law, if such information is compiled for law enforcement purposes and would, if disclosed:
(i) interfere with law enforcement investigations or judicial proceedings;
(ii) deprive a person of a right to a fair trial or impartial adjudication;
(iii) identify a confidential source or disclose confidential information relating to a criminal investigation; or
(iv) reveal criminal investigative techniques or procedures except routine techniques and procedures.

(b) When providing the data subject with access to information described in paragraph (b) of subdivision seven of section ninety-four of this article, an agency may withhold the identity of a source who furnished such information under an express promise that his or her identity would be held in confidence.

(6) Nothing in this section shall require an agency to provide a data subject with access to:
(a) personal information to which he or she is specifically prohibited by statute from gaining access;
(b) patient records concerning mental disability or medical records where such access is not otherwise required by law;
(c) personal information pertaining to the incarceration of an inmate at a state correctional facility which is evaluative in nature or which, if such access was provided, could endanger the life or safety of any person, unless such access is otherwise permitted by law or by court order;
(d) attorney’s work product or material prepared for litigation before judicial, quasi-judicial or administrative tribunals, as described in subdivisions (c) and (d) of section three thousand one hundred one of the civil practice law and rules, except pursuant to statute, subpoena issued in the course of a criminal action or proceeding, court ordered or grand jury subpoena, search warrant or other court ordered disclosure.

(7) This section shall not apply to public safety agency records.

(8) Nothing in this section shall limit, restrict, abrogate or deny any right a person may otherwise have including rights granted pursuant to the state or federal constitution, law or court order.

§96. Disclosure of records. (1) No agency may disclose any record or personal information unless such disclosure is:
(a) pursuant to a written request by or the voluntary written consent of the data subject, provided that such request or consent by its terms limits and specifically describes:
(i) the personal information which is requested to be disclosed;
(ii) the person or entity to whom such personal information is requested to be disclosed; and
(iii) the uses which will be made of such personal information by the person or entity receiving it; or
(b) to those officers and employees of, and to those who contract with, the agency that maintains the record if such disclosure is necessary to the performance of their official duties pursuant to a purpose of the agency required to be accomplished by statute or executive order or necessary to operate a program specifically authorized by law; or
(c) subject to disclosure under article six of this chapter, unless disclosure of such information would constitute an unwarranted invasion of personal privacy as defined in paragraph (a) of subdivision two of section eighty-nine of this chapter; or
(d) to officers or employees of another governmental unit if each category of information sought to be disclosed is necessary for the receiving governmental unit to operate a program specifically authorized by statute and if the use for which the information is requested is not relevant to the purpose for which it was collected; or
(e) for a routine use, as defined in subdivision ten of section ninety-two of this article; or
(f) specifically authorized by statute or federal rule or regulation; or
(g) to the bureau of the census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of Title XIII of the United States Code; or
(h) to a person who has provided the agency with advance written assurance that the record will be used solely for the purpose of statistical research or reporting, but only if it is to be transferred in a form that does not reveal the identity of any data subject; or
(i) pursuant to a showing of compelling circumstances affecting the health or safety of a data subject, if upon such disclosure notification is transmitted to the data subject at his or her last known address; or
(j) to a public archival facility as a record which has sufficient historical or other value to warrant its continued preservation by the state or for evaluation by the head of the archival facility or his or her designee to determine whether the record has such value; or
(k) to any person pursuant to a court ordered subpoena or other compulsory legal process; or

(l) for inclusion in a public safety agency record or to any governmental unit or component thereof which performs as one of its principal functions any activity pertaining to the enforcement of criminal laws, provided that, such record is reasonably described and is requested solely for a law enforcement function; or

(m) pursuant to a search warrant; or

(n) to officers or employees of another agency if the record sought to be disclosed is necessary for the receiving agency to comply with the mandate of an executive order, but only if such records are to be used only for statistical research, evaluation or reporting and are not used in making any determination about a data subject.

(2) Nothing in this section shall require disclosure of:

(a) personal information which is otherwise prohibited by law from being disclosed;

(b) patient records concerning mental disability or medical records where such disclosure is not otherwise required by law;

(c) personal information pertaining to the incarceration of an inmate at a state correctional facility which is evaluative in nature or which, if disclosed, could endanger the life or safety of any person, unless such disclosure is otherwise permitted by law;

(d) attorney's work product or material prepared for litigation before judicial, quasi-judicial or administrative tribunals, as described in subdivisions (c) and (d) of section three thousand one hundred one of the civil practice law and rules, except pursuant to statute, subpoena issued in the course of a criminal action or proceeding, court ordered or grand jury subpoena, search warrant or other court ordered disclosure.

§97. Civil remedies. (1) Any data subject aggrieved by any action taken under this article may seek judicial review and relief pursuant to article seventy-eight of the civil practice law and rules.

(2) In any proceeding brought under subdivision one of this section, the party defending the action shall bear the burden of proof, and the court may, if the data subject substantially prevails against any agency and if the agency lacked a reasonable basis pursuant to this article for the challenged action, award to the data subject reasonable attorneys' fees and disbursements reasonably incurred.

(3) Nothing in this article shall be construed to limit or abridge the right of any person to obtain judicial review or pecuniary or other relief, in any other form or upon any other basis, otherwise available to a person aggrieved by any agency action under this article.

§98. No waiver. Any agreement purporting to waive a data subject's rights under this article is hereby declared to be void as against public policy.

§99. Executive authority. Nothing in this article shall limit the authority of the governor to exercise his or her responsibilities.

§2. Severability. If any provision of article six-A of the public officers law, as added by this act, or the application thereof to any person or circumstances is adjudged invalid by a court of competent jurisdiction, such judgment shall not affect or impair the validity of the other provisions of such article or the application thereof to other persons and circumstances.

§3. Section eighty-nine of such law is amended by adding a new subdivision two-a to read as follows:

2-a. Nothing in this article shall permit disclosure which constitutes an unwarranted invasion of personal privacy as defined in subdivision two of this section if such disclosure is prohibited under section ninety-six of this chapter.

§4. This act shall take effect on the first day of September, nineteen hundred eighty-four; provided however, that agency actions necessary to the functioning of article six-A of the public officers law, as added by this act, on such date shall be taken prior thereto.
Sec. 315.1 Purpose and scope
315.2 Designation of privacy compliance officer
315.3 Proof of identity
315.4 Location
315.5 Hours for public inspection and copying
315.6 Requests for records
315.7 Amendment of records
315.8 Denial of request for a record or for amendment or correction of a record or personal information
315.9 Appeal
315.10 Statement of disagreement by data subject
315.11 Fees
315.12 Severability

Section 315.1 Purpose and scope.
(a) It is the responsibility and the intent of State University of New York to comply fully with the provisions of Article 6-A of the Public Officers Law, the "Personal Privacy Protection Law."

(b) The university shall maintain in its records only such personal information that is relevant and necessary to accomplish a purpose of the university that is required to be accomplished by statute or executive order, or to implement a program specifically authorized by law.
Personal information will be collected, whenever practicable, directly from the person to whom the information pertains.

The university will seek to ensure that all records pertaining to or used with respect to individuals are accurate, relevant, timely and complete.

These regulations provide information regarding the procedures by which members of the public may assert rights granted by the Personal Privacy Protection Law.

315.2 Designation of privacy compliance officer.

(a) The chancellor, for the central administration of the university, and the chief administrative officer of each State-operated institution are responsible for ensuring compliance with the regulations herein. For the purposes of central administration of the university, the Deputy to the Chancellor for Central Administration Services, or designee, State University Plaza, Albany, New York 12246, shall serve as privacy compliance officer. A privacy compliance officer shall be designated by the chief administrative officer of each State-operated campus. The name, title and business address of the campus privacy compliance officer may be obtained from the office of the chief administrative officer of each campus.

(b) Privacy compliance officers are responsible for ensuring appropriate responses to requests for access to and for amendment or correction of records in accordance with the Personal Privacy Protection Law. The designation of privacy compliance officers shall not be construed to prohibit officials who have in the past been authorized to make records available or to amend or correct such records from continuing to do so. Privacy compliance officers shall ensure that personnel:

(1) assist a data subject in identifying and requesting personal information, if necessary;

(2) describe the contents of systems of records orally or in writing in order to enable a data subject to learn if a system of records includes a record or personal information identifiable to the data subject;
(3) take one of the following actions upon locating the record sought:

   (i) make the record available for inspection, in a printed form without codes or symbols, unless an accompanying document explaining such codes or symbols is also provided;
   (ii) permit the data subject to copy the record; or
   (iii) deny access to the record in whole or in part and explain in writing the reasons therefor;

(4) upon request for copies of records, make a copy available upon payment of 25 cents per page;

(5) upon request, certify that a copy of a record is a true copy; or

(6) upon request, certify that:

   (i) the university or campus does not have possession of the record sought;
   (ii) the university or campus cannot locate the record sought after having made a diligent search; or
   (iii) the information sought cannot be retrieved by use of the description thereof, or by use of the name or other identifier of the data subject without extraordinary search methods being employed by the university or campus.

315.3 Proof of identity.

(a) When a request is made in person, or when records are made available in person following a request made by mail, the university or campus may require appropriate identification, such as a driver's license, an identifier assigned to the data subject by the university or campus, a photograph or similar information that confirms that the record sought pertains to the data subject.

(b) When a request is made by mail, the university or campus may require verification of a signature or inclusion of an identifier generally known only by a data subject, or similar appropriate identification.
c) Proof of identity shall not be required regarding a request for a record accessible to the public pursuant to the Freedom of Information Law.

315.4 Location. Records shall be made available at the office of the privacy compliance officer or at the location at which they are maintained. Whenever practicable, records shall be made available at an office near the residence of the data subject.

315.5 Hours for public inspection and copying. The university or campus shall accept requests for records and produce records during all regular business hours.

315.6 Requests for records.

(a) All requests shall be made in writing, except that the privacy compliance officer may make records available upon an oral request made in person after the applicant has demonstrated proof of identity.

(b) A request shall reasonably describe the record or records sought. Whenever possible, the data subject should supply identifying information that will assist in locating the records sought.

(c) Within five business days of the receipt of a request, the privacy compliance officer shall provide access to the record, deny access in writing explaining the reasons therefor, or acknowledge the receipt of the request in writing, stating the approximate date when the request will be granted or denied, which date shall not exceed thirty days from the date of the acknowledgment.

315.7 Amendment of records. Within thirty business days of a request from a data subject for correction or amendment of a record or personal information that is reasonably described and that pertains to the data subject, the privacy compliance officer shall:

(a) make the amendment or correction in whole or in part and inform the data subject that, on request, such correction or amendment will be provided to any person or governmental unit to which the record or personal information has been or is disclosed pursuant to Public Officers Law, §96(1)(d), §96(1)(i), or §96(1)(l); or
(b) inform the data subject in writing of his or her refusal to correct or amend the record, including the reasons therefor.

315.8 Denial of request for a record or for amendment or correction of a record or personal information.

(a) Denial of a request for records or for amendment or correction of a record or personal information shall be in writing, explaining the reasons therefor, and shall identify the person to whom an appeal may be directed.

(b) A failure to grant or deny access to records or to respond to a request for amendment or correction of a record within the time periods specified in sections 315.6 and 315.7 of this Part shall be construed as a denial which may be appealed.

315.9 Appeal.

(a) Any person denied access to a record or denied a request to amend or correct a record or personal information pursuant to section 315.8 of this Part may, within thirty business days of such denial, appeal to:

Vice Chancellor for University Affairs and Development, or designee
State University of New York
State University Plaza
Albany, New York 12246
Telephone: (518) 473-1825

(b) The time for deciding an appeal shall commence upon receipt of a written appeal identifying:

(1) the date and location of the request for a record or for amendment or correction of a record or personal information;

(2) the record that is the subject of the appeal; and

(3) the name and return address of the appellant.
(c) Within seven business days of an appeal of a denial of access, or within thirty business days of an appeal concerning a denial of a request for correction or amendment, the person designated to determine appeals shall:

(1) provide access to or correct or amend the record or personal information; or

(2) fully explain in writing the factual and statutory reasons for further denial and inform the data subject of the right to seek judicial review of such determination pursuant to Article 78 of the Civil Practice Law and Rules.

(d) If, on appeal, a record or personal information is corrected or amended, the data subject shall be informed that, on request, the correction or amendment will be provided to any person or governmental unit to which the record or personal information has been or is disclosed pursuant to Public Officers Law, §96(1)(d), §96(1)(i), or §96(1)(l).

(e) The person designated to determine appeals shall immediately forward to the Committee on Open Government a copy of any appeal made pursuant to this Part, the determination thereof, and the reasons therefor.

315.10 Statement of disagreement by data subject.

(a) If correction or amendment of a record or personal information is denied in whole or in part upon appeal, the person designated to determine appeals shall inform the data subject of the right to:

(1) file with the university a statement of reasonable length setting forth the data subject's reasons for disagreement with the determination;

(2) request that such a statement of disagreement be provided to any person or governmental unit to which the record has been or is disclosed pursuant to Public Officers Law, §96(1)(d), §96(1)(i), or §96(1)(l).

(b) Upon receipt of a statement of disagreement by a data subject, the university shall clearly note any portions of the record that are disputed and attach the data subject's statement as part of the record.
(c) When providing a data subject's statement of disagreement to a person or governmental unit in conjunction with a disclosure made pursuant to Public Officers Law, §96(1)(d), §96(1)(i), or §96(1)(l), the university may also include a concise statement of its reasons for not making the requested amendment or correction.

315.11 Fees

(a) Unless otherwise prescribed by statute, there shall be no fee charged for:

(1) inspection of records;

(2) search for records; or

(3) any certification pursuant to this Part.

(b) Unless otherwise prescribed by statute, copies of records shall be provided:

(1) upon payment of 25 cents per page; or

(2) upon payment of the actual cost of reproduction, if the record or personal information cannot be photocopied.

315.12 Severability. If any provision of this Part or the application thereof to any person or circumstances is adjudged invalid by a court of competent jurisdiction, such judgment shall not affect or impair the validity of the other provisions of this Part or the application thereof to other persons and circumstances.