

# Information Privacy and Security

---

<b>PURPOSE</b> .....	<b>1</b>
<b>POLICY</b> .....	<b>2</b>
<b>WHO SHOULD KNOW THIS POLICY</b> .....	<b>2</b>
<b>DEFINITIONS</b> .....	<b>3</b>
<b>REGULATIONS</b> .....	<b>3</b>
1.0 COLLECTION OF CONFIDENTIAL INFORMATION.....	3
1.1 <i>Information Associated with "Identity Theft"</i> .....	4
1.2 <i>Individuals' Rights</i> .....	4
2.0 PROTECTION OF CONFIDENTIAL INFORMATION .....	4
2.1 <i>Responsibilities of Information Security Officers</i> .....	5
2.1.1 <i>Assessing Security Requirements</i> .....	6
2.2 <i>Responsibilities of Record Custodians</i> .....	7
2.2.1 <i>Information Privacy and Safeguarding Plans</i> .....	7
2.2.2 <i>Record Retention and Destruction</i> .....	8
2.2.3 <i>Additional Requirements for Technology Managers</i> .....	8
2.3 <i>User Responsibilities</i> .....	9
2.4 <i>Service Provider Requirements</i> .....	10
2.4.1 <i>Due Diligence of Service-Providers</i> .....	10
3.0 ACCESS TO CONFIDENTIAL INFORMATION .....	10
3.1 <i>Electronic Access to Confidential Information</i> .....	10
4.0 PERMITTED DISCLOSURES OF CONFIDENTIAL INFORMATION .....	11
4.1 <i>Exchanging Information via E-Mail or Other Network Facilities</i> .....	11
4.2 <i>Subpoenas</i> .....	12
5.0 REQUIRED DISCLOSURE OF SECURITY BREACH .....	12
5.1 <i>California Security Breach Notification Act</i> .....	12
6.0 TRAINING .....	13
7.0 PERIODIC EVALUATION AND REVISION.....	13
<b>FORMS</b> .....	<b>13</b>

## Purpose

The purpose of ASI's Policy on Information Privacy and Security is to define the principles to which all directors, officers, agents, and employees of the Associated Students, Incorporated (ASI) must adhere when handling confidential information owned by or entrusted to Associated Students, Incorporated in any form. These principles cover the following areas:

- Defining the confidentiality, integrity and availability requirements for information used to support ASI's operations,

- Ensuring that those requirements are effectively communicated to individuals who come in contact with such information, and
- Using, managing, and distributing such information – whether electronically or physically - in a manner that is consistent with those requirements

The following describes in general terms ASI's Information Privacy and Security Policy, which is also embodied in various information privacy and security plans developed by the custodians of specific information.

## Policy

It is the policy of the Associated Students, Incorporated that all information gathered and maintained by directors, officers, agents and employees of Associated Students, Incorporated for the purpose of conducting ASI business is considered corporate information. As such, each individual who uses, stores, processes, transfers, administers and/or maintains this information is responsible and shall be held accountable for its appropriate use. In summary, anyone who handles such information shall:

- Abstain from divulging, copying, releasing, selling, loaning, reviewing, altering or destroying any information except as properly authorized within the scope of one's professional activities and authority.
- Take appropriate measures to protect confidential information wherever it is located, e.g., held on physical documents, stored on computer media, communicated over voice or data networks, exchanged in conversation, etc.
- Safeguard any physical key, ID card, or computer/network account that permits access to confidential information. This includes creating computer passwords that satisfy the requirements of ASI's Policy on Computing Resources.
- Render unusable any confidential information held on any physical document or computer storage medium (e.g., diskette, CD, magnetic tape, hard disk) that is being discarded.
- Report any activities that may compromise confidential information to their immediate supervisor or to the appropriate Information Security Officer.

## Who Should Know This Policy

- |  |  |   |
|--|--|---|
| <input checked="" type="checkbox"/> Budget Area Administrators | <input checked="" type="checkbox"/> Elected/Appointed Officers | <input type="checkbox"/> Grant Recipients |
| <input checked="" type="checkbox"/> Management Personnel       | <input checked="" type="checkbox"/> Program Advisors           | <input checked="" type="checkbox"/> Staff |
| <input checked="" type="checkbox"/> Supervisors                | <input checked="" type="checkbox"/> Volunteers                 |   |

## Definitions

For purposes of this policy, the terms used are defined as follows:

Term	Definition
Access	Personal inspection or review of confidential information or a copy of confidential information, or an oral or written description or communication of confidential information
Confidential Information	Information that identifies or describes an individual, including, but not limited to, his or her social security number, physical description, home address, home telephone number, ethnicity, gender, telephone number, signature, passport number, bank account number, education, financial matters, medical or employment history, and performance evaluations. It includes statements made by, or attributed to, the individual. It also includes computerized data that includes an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social Security number; (2) driver's license number or California Identification Card number; (3) account number (which could include a student or employee identification number), credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account. Confidential Information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. Confidential Information does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, such as name, address, or telephone number.
Disclosure	To permit access to or to release, transfer, disseminate, or otherwise communicate all or any part of confidential information by any means, orally, in writing, or by electronic or any other means to any person or entity
Financial Information	Financial Information includes but is not limited to information about an individual's number of tax exemptions, amount of taxes withheld, amount of OASDI withheld, amount and type of voluntary/involuntary deductions/reductions, survivor's amounts, net pay and designee for last payroll warrant
Handled	The access, collection, distribution, process, protection, storage, use, transmittal, or disposal of information containing confidential data
Information Security Officer	The individual or individuals responsible for protecting: (1) confidential information in the custody of ASI; (2) the security of the equipment and/or repository where this information is processed and/or maintained; and (3) the related privacy rights of the students and staff concerning this information
Permitted Disclosures	Disclosures of confidential information permitted under the California Information Practices Act of 1977
Record Custodian	The individual with responsibility for maintenance of a repository of records
Service Provider	Any person or entity that receives, maintains, processes, or otherwise is permitted access to confidential information through its provision of service directly to ASI
Third Party	Any individual (or individual on behalf of an organization) who is not an employee of ASI

## Regulations

### 1.0 Collection of Confidential Information

Confidential information shall not be collected unless it is appropriate and relevant to the purpose for which it will be collected. It must be collected, to the extent possible, from the individual directly and not from other sources. Where information is obtained from other sources, a record must be maintained of those sources from which the confidential information was obtained.

There shall be no confidential information collected or maintained which has not been approved by the appropriate Information Security Officer. Personal information shall not be transferred outside

the Associated Students, Incorporated unless the transfer is compatible with the disclosed purpose for which it was collected.

### 1.1 Information Associated with "Identity Theft"

Collection and use of any of the following pieces of information shall be limited to situations where there is legitimate business need and **no reasonable alternative exists**. Department supervisors must ensure that their employees understand the need to safeguard this information, and that adequate procedures are in place to minimize this risk. Access to such information may only be granted to authorized individuals on a need to know basis.

- Social Security Number
- Date of birth
- Credit card numbers
- Bank account numbers
- Drivers license numbers

The following information associated with identity theft shall not be collected or maintained under any circumstances:

- Place of birth
- Mother's maiden name
- Income tax records

### 1.2 Individuals' Rights

Individuals have the right to inquire and be notified about whatever confidential information ASI maintains concerning them. An opportunity to inspect any such confidential information must be afforded within 30 days of any request. If the record containing the confidential information also contains confidential information about another individual, that information must be deleted from the record before it is disclosed. Individuals may request copies of records containing any confidential information about them, and those copies must be provided within 15 days of the inspection. ASI may charge a reasonable per page cost for making any copies. Individuals may request that their personal information be amended and, if the request is denied, the individual may request a review of that decision by the Executive Director or designee.

## 2.0 Protection of Confidential Information

ASI-held information shall be protected against unauthorized exposure, tampering, loss, and destruction, wherever it is found, in a manner that is consistent with applicable federal and state laws and with the information's significance to the ASI and any individual whose information is collected. Achieving this objective requires that ASI information be segregated into logical collections (e.g., employee benefit data, payroll data, personnel records, volunteer data, personal data regarding donors, financial records), and that each collection be associated with an individual known as an "Information Security Officer".

The following table identifies the Information Security Officers currently assigned to information collections maintained by ASI.

Information Collections Pertaining to	Information Security Officer	Record Custodian
<b>STUDENTS</b>		
Applications for Employment	Human Resources Manager	Human Resources Technician
Applications for Government Office	Executive Director	Student Government Advisor
Childcare Records, including enrollment, immunization, injury reports, development reports, parent information, etc.	Director, Child Development Center	CDC Administrative Specialist
Scholarship Applications	Executive Director	Development Associate
Student Assistant Personnel Files	Human Resources Manager	Human Resources Technician
Student Health Insurance Enrollment	Executive Director	Executive Director
Volunteer Applications	Executive Director	Executive Assistant
Volunteer Service Records	Executive Director	Executive Assistant
<b>STAFF</b>		
Applications for Employment	Human Resources Manager	Human Resources Technician
Dependents and beneficiaries of current staff	Human Resources Manager	Human Resources Technician
Employee Benefits Data	Human Resources Manager	Human Resources Technician
Payroll Records	Human Resources Manager	Human Resources Technician
Personnel Files	Human Resources Manager	Human Resources Technician
<b>ALUMNI AND DONORS</b>		
ASI Alumni Information	Executive Director	Development Associate
Donor Records	Executive Director	Development Associate
Gifts and Donations	Executive Director	Development Associate
<b>FINANCIAL MATTERS</b>		
Accounts Receivable Customer Files	Controller	Accounts Receivable Technician
Accounts Payable Vendor Files	Controller	Expenditures Technician
Financial Aid Recipients	Controller	Expenditures Technician
<b>LEGAL MATTERS</b>		
Insurance Claims	Executive Director	Controller
Legal Opinions	Executive Director	Executive Director
Litigation	Executive Director	Executive Director
Legal Settlements	Executive Director	Executive Director
Tax Returns	Controller	Staff Accountant

## 2.1 Responsibilities of Information Security Officers

Each Information Security Officer may designate one or more individuals on his or her staff to perform the following duties. However, the Information Security Officer retains ultimate responsibility for the following actions.

- Defining the collection's requirements for confidentiality, integrity and availability
- Develop department Information Privacy and Safeguarding Plans (see below) that support the objectives for confidentiality, integrity and availability defined by the

Information Security Officers and their designees and ensure that those procedures are followed

- Effectively communicate any restrictions to those who use, administer, process, store, or transfer the information in any form, physical or electronic
- Ensure that each staff member understands his or her information security-related responsibilities and acknowledges that he or she understands and intends to comply with those requirements by having them review and sign the “Protection of Confidential Information – Summary of Responsibilities” document
- Work with Record Custodians to determine what users, groups, roles, or job functions are authorized to access the information in the collection and in what manner (e.g., who can view the information, who can update the information).
- Convey the collection’s requirements in writing to the supervisors of departments that will have access to the collection,

#### 2.1.1 Assessing Security Requirements

To facilitate the assessment process and ensure that security requirements are expressed in a consistent manner, Information Security Officers and their designees will be required to categorize their information collections using the following guidelines.

The **confidentiality** requirement for an information collection will be expressed in the following terms:

- **“Public”** information can be freely shared with individuals on or off campus without any further authorization by the appropriate Information Security Officer or designee.
- **“Internal”** information can be freely shared with directors, officers, agents and employees of ASI. Sharing such information with individuals outside of ASI requires authorization by the appropriate Information Security Officer or designee.
- **“Departmental”** information can be freely shared with members of the owning department. Sharing such information with individuals outside of the owning department requires authorization by the appropriate Information Security Officer or designee.
- **“Confidential”** information can only be shared on a “need to know” basis with individuals who have been authorized by the appropriate Information Security Officer or designee, either by their association with specific job functions or explicitly by name.
- **“Highly confidential”** information can only be shared on a “need to know” basis with a limited number of individuals who have been authorized by the appropriate Information Security Officer or designee explicitly by name.

The **integrity/availability** requirement for an information collection will be expressed as follows:

- **“Non-critical”** if its unauthorized modification, loss or destruction would cause little more than temporary inconvenience to the users and support staff, and incur limited recovery costs. Reasonable measures to protect information deemed “non-critical” include storing physical information in locked cabinets and/or office space, using standard access control mechanisms that prevent unauthorized individuals from updating computer-based information, and making regular backup copies.
- **“Critical”** if its unauthorized modification, loss, or destruction through malicious activity, accident or irresponsible management could potentially cause the ASI to:
  - Suffer significant financial loss or damage to its reputation,
  - Be out of compliance with legislative requirements,
  - Adversely impact its clients, or
  - Miss a legally mandated deadline.

In addition to the protective measures described for information deemed “non-critical”:

- “Critical” information must be verified either visually or against other sources on a regular basis, and
- A business continuity plan to recover “critical” information that has been lost or damaged must be developed, documented, deployed and tested annually.

## 2.2 Responsibilities of Record Custodians

Record Custodians are required to:

- Understand the security-related requirements for the information collections in their possession by working with the appropriate Information Security Officers
- Determine and implement methods to protect all printed material containing confidential information against destruction, loss, or damage from potential environmental hazards such as fire or water damage to the extent possible
- Report any evidence that information has been compromised or any suspicious activity that could potentially expose, corrupt, or destroy information to the appropriate Information Security Officer and the Executive Director, or to the university internal auditor

### 2.2.1 Information Privacy and Safeguarding Plans

The development and implementation of written information privacy and safeguarding plans is the responsibility of each Information Security Officer. The plan must be dated and signed and must include at a minimum the following information:

- Name of the office, department, or operation where confidential information is handled;

- Name of the record series (files) containing confidential information;
- Identification of confidential information handled;
- Names and titles of individuals with access to confidential information;
- Administrative controls implemented to minimize the number of individuals with access to confidential information;
- Description of methods to physically secure records;
- Discussion of records retention and destruction methods; and
- Discussion of training content, frequency, delivery method, etc.

### 2.2.2 Record Retention and Destruction

The maintenance of records beyond the retention requirements set forth in ASI's Records Retention and Disposition Schedule presents a significant risk to the security and integrity of confidential information. Unless a longer retention is specifically approved by the Executive Director, records containing confidential information shall be destroyed within 3 months following the required period of retention.

Record destruction is the responsibility of Information Security Officers. All printed material containing confidential information shall be destroyed when retention is no longer required. Destruction must prevent unauthorized access to confidential information (i.e., shredding).

Prior to the survey and disposal of an ASI computer or the transfer of a computer from one ASI user to another user, the computer's hard drive shall be wiped clean using a low level format utility to remove the operating system, software applications installed on the computer and any personal files which were stored on the computer.

Questions regarding desktop security procedures may be directed to the ASI Systems Administrator.

### 2.2.3 Additional Requirements for Technology Managers

Technology managers are those department supervisors who manage computing and network environments where ASI information is stored, transmitted or processed, such as:

- Computer operating environments (e.g., Windows, Macintosh, etc.)
- Database management environments (e.g., SQL Server, Access, etc.)
- Application environments (e.g., Abra, MAS 200, Private Advantage, etc.),
- Network environments (e.g., electrical, optical, microwave and wireless networks, routers, switches, firewalls, etc.),
- Physical storage facilities (e.g., tape libraries, filing cabinets, etc.),

Technology managers are responsible for ensuring that specific data's requirements for confidentiality, integrity and availability as defined by the appropriate Information Security Officer are being satisfied within their environments. This includes the development of:

- A cohesive architectural policy,
- Product implementation and configuration standards,
- Procedures and guidelines for administering network and system accounts and access privileges in a manner that satisfies the security requirements defined by the Information Security Officers, and
- An effective strategy for protecting information against generic threats posed by computer hackers.

### 2.3 User Responsibilities

Each individual who has access to information owned by or entrusted to the ASI is expected to know and understand its security requirements and to take measures to protect the information in a manner that is consistent with the requirements defined by this policy, wherever the information is located, specifically

- On printed media (e.g., forms, reports, microfilm, microfiche, books)
- On computers
- On networks (data and voice)
- On magnetic or optical storage media (e.g., hard drive, diskette, tape, CD)
- In physical storage environments (e.g., offices, filing cabinets, drawers)
- In a person's memory, etc.

If an authorized user is not aware of the security requirements for information to which he or she has access, he or she must provide that information with maximum protection until its requirements can be ascertained.

Any individual who has been given a physical key, ID card, or logical identifier (e.g., computer or network account) that enables him or her to access information is responsible for all activities performed by anyone using that key or identifier. Therefore, each individual must be diligent in protecting his or her physical keys and ID cards against theft, and his or her computer and network accounts against unauthorized use. Passwords created for computer and network accounts should be difficult to guess (see "Policy on Computing Resources" document for guidelines). Furthermore, passwords should never be shared or recorded and stored in a location easily accessible by others. The assignment of a single network or system account to a group of individuals sharing the same password is highly discouraged and may only occur in cases where there is no reasonable, technical alternative.

Stolen keys and ID cards, and computer and network accounts suspected of being compromised should be reported to the appropriate Information Security Officer immediately.

## 2.4 Service Provider Requirements

Due to the specialized expertise needed to design, implement, and service new technologies, vendors may be needed to provide resources that ASI is unable to provide on its own. Further, vendors may be needed to assist in the disposal of the volumes of hard-copy confidential information that is generated by ASI. In recognition of its responsibility for the performance and actions of these vendors, the following actions are required:

### 2.4.1 Due Diligence of Service-Providers

The adequacy of the service provider's system of safeguarding information shall be determined by the Controller prior to ASI entering into a contractual relationship with the service provider. ASI shall not contractually engage a service provider who cannot demonstrate that they have a system to safeguard student, employee, or donor information. ASI shall not enter into a contractual agreement with any provider who is not capable of maintaining appropriate safeguards for confidential information.

### 2.4.2 Service Provider Agreements

All contracts with service providers must include a privacy clause that requires the service provider to implement appropriate measures to safeguard confidential information and to refrain from sharing any such information with any other party. In those cases where the service provider's contract does not include a privacy clause, a Confidential Information Addendum must be completed and appended to the service provider's contract.

Contracts must, when appropriate, include the requirement that in addition to the ASI insurance requirements for service agreements, the service provider be bonded and maintain personal liability insurance that protects against allegations of violations of privacy rights of individuals as a result of improper or insufficient care on the part of the service provider.

## 3.0 Access to Confidential Information

No ASI director, officer, or employee shall be granted access to confidential information in ASI's custody without the review and written approval of the appropriate Information Security Officer. The approval of access to confidential information will be based on several factors including the determination that access is required for the employee to perform a critical function that is part of the employee's job duties and responsibilities and assurance that all requirements designed to protect individual privacy and safeguard confidential information will be met.

Employees approved for security access must receive appropriate training and sign a "Protection of Confidential Information – Summary of Responsibilities document". A copy of the signed form will be retained in the individual's official personnel file. Additionally, copies of the signed form should be kept on file with the appropriate department supervisor.

### 3.1 Electronic Access to Confidential Information

Employees needing access to confidential information stored on network servers or computers must complete a Network Account Request form and have it approved by their supervisor and the appropriate Information Security Officer. The employee will be assigned an account by the Systems Administrator. Accounts will be immediately deactivated upon the separation of the employee. An employee approved for access to electronic information does not need to complete an additional form for access to the same information in a non-electronic format.

#### 4.0 Permitted Disclosures of Confidential Information

The California Information Practices Act, enacted in 1977 prohibits disclosure of personal information except in certain limited circumstances. Consultation with the Executive Director is required before releasing personal information covered by the Information Practices Act.

The more common exceptions permit disclosure in the following circumstances:

- To the individual to whom the information pertains;
- Where the individual to whom the information pertains has given voluntary written consent to disclose the information to an identified third party no more than 30 days before the third party requested it, or within the time limit agreed to by the individual in the written consent;
- To an appointed guardian or conservator or a person representing the individual provided it can be proven with reasonable certainty through ASI forms, documents or correspondence that the person is the authorized representative of the individual to whom the information pertains;
- To persons within the ASI who need the information to perform their functions;
- To another government agency when required by law;
- In response to a request for records under the California Public Records Act (unless the Public Records Act provides an exception);
- Where there is advance written assurance that the information is to be used for purposes of statistical research only and where the information will be redisclosed in a form that does not identify any individual;
- Where ASI has determined that compelling circumstances exist which affect the health or safety of the individual to whom the information pertains, and notification is transmitted to the individual at his or her last known address, and disclosure does not conflict with other state or federal laws;
- Pursuant to a subpoena, court order, or other compulsory legal process if, before disclosure, ASI notifies the individual to whom the record pertains, and if the notification is not prohibited by law;
- Pursuant to a search warrant;
- To a law enforcement or regulatory agency when required for an investigation of unlawful activity of or for licensing, certification, or regulatory purposes, unless the disclosure is otherwise prohibited by law.

#### 4.1 Exchanging Information via E-Mail or Other Network Facilities

Electronic mail (e-mail) may in some situations be considered an insecure mechanism for exchanging information. The privacy of information contained within e-mail messages can be exposed, especially when either the sender or any of the recipients are off-campus or utilize a wireless network connection. The use of mechanisms that exchange information in a readable form, such as "ftp", "chat" and "instant messaging", between on- and off-campus computers

also places confidential information at risk. If information, deemed by its Information Security Officer as “confidential” or “highly confidential”, must be exchanged with an individual or entity off-campus using e-mail or any other network facility that transfers data, it must be encrypted using a hardware- or software-based mechanism approved by the Systems Administrator.

All business-related e-mail containing “confidential” or “highly confidential” information sent to recipients who are not in the “csulb.edu” domain must include the following disclaimer:

“This electronic communication, including any attached documents, may contain confidential and/or legally privileged information that is intended only for use by the recipient(s) named above. If you have received this communication in error, please notify the sender immediately and delete the communication and any attachments.”

#### 4.2 Subpoenas

Authorized users are reminded that the full range of information collected on any living or deceased individual – students, faculty, staff, alumni, parents, custodians, spouses, children, donors, beneficiaries, etc. – in hard copy or electronic form may be subpoenaed and entered into the public record of a court case. Appropriate discretion should therefore be exercised in the drafting of any document that will be stored in any ASI file. Employees who receive investigative subpoenas, court orders and other compulsory requests from law enforcement agencies that require the disclosure of ASI held information should contact the Executive Director before taking any action.

### 5.0 Required Disclosure of Security Breach

ASI is required to disclose any breach of system security to individuals whose unencrypted personal information was, or is reasonably believed to have been acquired by an unauthorized person. Any student, staff, or other agent having access to ASI confidential information shall immediately notify the appropriate Information Security Officer and the Executive Director, or the university Internal Auditor. The Executive Director or the university Internal Auditor shall, without unreasonable delay, notify the CSU Office of General Counsel.

#### 5.1 California Security Breach Notification Act

In an attempt to stem the growth of identity theft, the State of California enacted the California Security Breach Notification Act which mandates the public disclosure of computer security breaches in which confidential information of any California resident may have been acquired, or reasonably believed to have been acquired, by an unauthorized person. Although the definition of confidential information contained in various pieces of legislation is very broad, the definition of confidential information as used in the California Security Breach Notification Act is quite narrow.

Under this act, confidential information means an individual's first name or initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

- Social security number or last 4 digits of SSN with date of birth (DOB);

- Driver's license number or California Identification Card number;
- Account number (including student identification number), credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Any ASI employee who believes that a security breach has occurred shall immediately notify the CSULB Vice President, Administration and Finance and the CSULB Information Security Officer at (562) 985-8260. After business hours, notification shall be made to University Police, (562) 985-4101.

## 6.0 Training

All ASI directors, officers, and employees having access to confidential information will receive training regarding ASI's Policy on Information Privacy and Security and the Information Privacy and Safeguarding Plan for their department or administrative unit. Employee training shall be provided by the appropriate Information Security Officer. Information Security Officers and Record Custodians shall keep documentation of this training for review by the university internal auditor.

## 7.0 Periodic Evaluation and Revision

ASI shall periodically evaluate, test, and adjust the confidential information security program to validate that equipment and systems function properly and produce the desired results. Each Information Security Officer and department supervisor shall perform ongoing assessments to ensure that employees follow written procedures for information security. Information security shall be included in all internal audits. ASI shall conduct periodic reviews of the Policy on Information Privacy and Security to ensure that it remains appropriate and relevant.

## Forms

The following forms and procedures are to be used in the execution of this policy.

Form Name	Purpose	Responsible Office	Approved By	Timeline for Submission
Confidential Information Addendum	To amend a service provider's contract to include a privacy clause requiring the service provider to implement appropriate measures to safeguard confidential information and to refrain from sharing any such information with any other party	A.S. Business Office	Executive Director	Must be completed and fully executed prior to the exchange of any confidential information
Information Privacy and Safeguarding Plan	To disclose the location of confidential information held by ASI offices and document controls over access, physical security, retention, and destruction	Office of the Executive Director	Information Security Officer	Must be initially completed by 09/30/05 and updated whenever changes in personnel or practices occur
Protection of Confidential Information – Summary of Responsibilities	To request approval for employee access to confidential information maintained by ASI and to document their training in and understanding of security requirements	Office of the Executive Director	Information Security Officer	Must be completed and fully executed prior to providing access to the employee.

Form Name	Purpose	Responsible Office	Approved By	Timeline for Submission
Network Account Request	To request access to data or other resources located on one or more of ASI's network servers	Systems Administration	Division Director and Executive Director	Minimum of 3 business days before desired date of account activation