ASPEN CENTER FOR PHYSICS

INFORMATION SECURITY POLICY

Information Security Policy

Procedure Sections

- **Reason for Procedure**
- **Who Should Know This Procedure**
- **Contacts**
- **Applicable ACP Policies**
- **Information Security Policy at ACP**
- **Roles & Responsibilities**
- **Appendix: Applicable Federal Regulations & Criteria**

Last Revised: July 2012

Responsible Member
Computer Chair

Reason for Procedure

This procedure outlines the policies and processes for the protecting sensitive information including credit card information at the Aspen Center for Physics.

Who Should Know This Procedure

- ☐ Principal Investigators
- ☑ Administrative Staff
- ☐ Winter Conference/Summer Workshop Organizers
- ☐ Proposal Committee
- ☐ Officers
- ☐ Trustees
- ☐ General Members
- ☑ IT Firm that manages the ACP network
- ☑ Computer Committee

Contacts

Subject	Contact
Information Security Questions	Finance Manager Computer Committee

Applicable ACP Policies

- None

Information Security Policy at ACP

Information Security Manager: Finance Manager
ACP 700 West Gillespie, Aspen, CO 81611 * 970-925-2585

We are a conference/workshop center in Aspen, Colorado. We have a credit card machine at our front desk and use online credit card services for deposits prior to arrival.

What is Sensitive Information?

Sensitive information is information that is not lawfully available to the public and could be used to damage our participants, our employees, or our business. This includes personal information most commonly used to commit identity theft and similar crimes, such as a person's name and any of the following:

- Personal identification, including: a number or other identifying information from social security, state id card, driver's license, passport, employee id
- Financial account identification, including: bank account number or credit card number
- Other identifying information to access financial accounts or non-public records, including: usernames, passwords, PINs, etc.
- Employee records, including payroll, pension, and insurance
- Business-private information for legitimate business purposes, including business plans; vendor and customer lists; contracts; and account information of vendors, clients, and customers
- Financial transactions with our customers, employees, and vendors, including cash, check, and credit card transactions

Why We Need Sensitive Information

Customers, employees, vendors, and business partners entrust sensitive information to us for good business reasons. We store and use that information responsibly, protecting it from unauthorized or illegal use.

Here are some ways we use it:

- As required by law, we keep employment records, including payroll records, and tax forms (W-4 and I-9).
- When a customer pays by credit card we normally don't record the credit card number (we just swipe the card through the reader), but if the reader is broken we record the credit

card information and deliver it to our credit card processing service. If a payer phones in the credit card number we write it down and process it in the credit card machine.

Storage And Display of Sensitive Information

Sensitive information can be stored and displayed on many kinds of media.

- Many of these media are casually removable and portable, including paper, CD, DVD, external hard drives, and flash drives
- Other media are not as casually removable, including computer internal hard drives

All media are subject to theft by someone who:

- Breaks or bypasses the visual security of the store or home office, including seeing computer screens, checks, and credit slips of other people
- Breaks or bypasses the physical security of the building
- Breaks or bypasses the electronic security of our computers and networks

It is our responsibility to make it reasonably difficult for someone to gain access to sensitive information in our possession.

Sharing Senstive Information With Government Organizations

As a rule, we do not share sensitive information with government agencies. If we have to share anything sensitive we assume the government will follow information security policies that are legally compliant and over which we have no control.

Sharing Financial Information With Financial Institutions

We routinely share sensitive financial transaction information with our financial institutions, including customer checking account numbers and credit card numbers.

Sharing Sensitivite Information With ISP-Compliant Vendors

We routinely share sensitive information in the form of employment records, pension and insurance information, and other information required to be a responsible employer.

We might share this with our CPA firm, our legal counsel, and our investment advisor.

Each year, we require each of these organizations to confirm in writing that they follow a written Information Security Plan that fully complies with all governmental laws and regulations for this location, signed by the CEO or other authorized person.

Ensuring That Our Staff Follows Our Information Security Policy

Our Information Security Manager (ISM) trains every new member of our staff in his or her role in carrying out the Information Security Policy (ISP). This training is refreshed at least annually. New staff members agree in writing to follow our ISP, and understand that their continued employment in our organization depends on their following the ISP. Employees who fail to follow the ISP are given written warnings, followed, if necessary, by being asked to leave the organization.

Protection of Senstive Information

We use good common-sense practices to protect sensitive information:

- We keep all unencrypted and easily removable physical media that contains sensitive information (check, credit slip, CD, DVD, tape, flash drive, paper, microform, etc.) in a locked space where it is reasonably safe from burglary and intrusion.
- When we use sensitive information, we hold the media and its contents closely, we don't share it inappropriately, and we return it to an appropriate locked space when we're done. For example, we don't leave lying on counters, tables, or desks any unencrypted sensitive information, including checks, credit slips, and file folders containing W-4s and I-9s. We also don't leave sensitive information displayed on an unattended computer screen.
- All client information is maintained onsite within the office network.

- Backups go to physical hard drives which are kept in a locked room within the locked basement.

- No client data is ever transferred offsite over the internet except with an encrypted connection to our accounting cloud service. No credit card information is ever transmitted over the internet. Physicist names, addresses, and history at ACP, are transmitted with password protection to and from the Center's offsite database

Destruction of Obsolete Sensitive Information

We regularly destroy obsolete records

- We destroy most paper records using an office-grade shredder
- We destroy most records on re-writeable media (disk drives, flash drives, etc.)
- We destroy other records in media-appropriate ways, such as physical breakage or delivery to an ISP-compliant information destruction service

Usernames And Passwords

- Usernames and passwords may only be delivered together by hand
- Usernames and passwords may both be delivered by mail only if they are mailed on different days
- Otherwise, usernames may only be delivered separately by a route of hand, fax, phone, mail, or email; and passwords may only be delivered separately by a different route of hand, fax, phone, or mail. Passwords for physicists' access to their ACP database record which contains no vital personal numbers is an exception and is delivered by email

Financial Transactions

- When we receive checks from participants or donors, we keep them in a locked space. Usually the Administrative Vice President or the Front Desk prepares a bank deposit. The paper deposit slip with backup is given to the Finance Manager
- Administrative Vice President, Front Desk Manager or Finance Manager delivers checks,

cash, and other financial instruments by hand to an appropriate financial institution, which at present is Alpine Bank
- Unencrypted employment records are kept in a locked space, and accessed only by the staff responsible for employment issues
- Unencrypted records with sensitive information are never removed from the ACP front offices except to be stored in double-locked archives in the basement of ACP Smart Hall or to be examined on property by our CPA auditor

Emailing Sensitive Information

We email sensitive information between us and our payroll and pension companies and accountant, only in strongly encrypted form with a password arranged by in-person, fax, or telephone contact.

Strong Passwords

Password must be at least 8 characters, including one punctuation mark and one change of case. The password must be hard to crack by a dictionary attack, so if it has a word or a proper name, it must have at least TWO unrelated words or proper names.

The ISM keeps all passwords in a master password file that is shared by the Adm VP and the Front Desk Manager. The password list includes the administrator password for all our PCs and servers.

The workstation administrator passwords are changed when security urgently requires it, such as when a senior staff person leaves on bad terms.

No Unencrypted Sensitive Information

We do not keep sensitive information on laptops, or other handheld or portable devices.

Network Security (provided by ACP's IT Consultant)

- Email services which include spam/malware filtering are contracted and provided offsite by an off-site provider
- Aspen Center for Physics public facing DNS and web site hosting are provided offsite by an off-site provider
- Office network (where any potentially sensitive information might be stored) is 100% firewalled and on an entirely different subnet from the Center's public/guest/wifi network
- Firewall Integrity is validated periodically using nmap network scans
- No wifi access is present on the office network, it's wired only
- Office LAN is on dedicated switch partitions, and is physically accessible only within the office area, and the locked data center controlled by the staff

- Local DNS caching servers are configured to protect against cache injection, meaning they will pass the grc test
- Passwords/access to the office computers managed by the end user - so when an employee quits, passwords will be changed by the ISM
- Office computers and network are kept secure behind locked doors with access limited to staff
- The network is monitored 24x7 for performance/reliability, and the ACP IT consultant gets emails if there are any anomalies
- Network firewall servers are updated bi-annually, and emergency security patches may be applied immediately if needed
- Remote administrative access is provided by ssh

Computer Security

When a new computer is added to our network, it is secured with passwords. Data is removed from old computers.

When a Staff Person Leaves Our Organization

When a staff person leaves our organization, all passwords that person used are changed, so that the person no longer has access to our computer network remotely or if s/he visits the office. The person also returns any keys used to physically secure PI.

We keep regular computer backups on and offsite.

If a Breach Occurs

If our ISM determines that sensitive information has been stolen, the ISM will notify the Office of Consumer Affairs & Business Regulation (OCABR) and the Attorney General's Office, describing the theft in detail, and work with authorities to investigate the crime and to protect the victim's identity and credit. To the extent possible, our ISM will also warn the victims of the theft so that they can protect their credit and identities.

- Computer Security:
  - Everyone must enter a correct username-password pair to access one of our computers
  - Operating System set to automatically download and install security updates
  - Antivirus configured to download and install both code and virus signature updates
  - If computers seem to be slow or otherwise not working normally, the staff runs scans on

the computer. If the problem persists, the ISM contacts the computer helping service

- Anti-phishing and poisoned website measures

Roles & Responsibilities

Administrative Vice President Accounts Receivable, Employment, and Information Security. Deliver checks to the bank. Billing.

Front Desk Manager: Deliver checks to the bank. Responsibilities assigned by the Administrative Vice President. Work with customers, perform financial transactions, follow Information Security Plan and other policies of the organization.

Information Security Manager: Security Plan; train new staff and refresh training of all staff on information security; regularly audit staff and vendor on information security compliance. Deliver checks to the bank and other responsibilities assigned by the Administrative Vice President. Work with physicists, perform financial transactions, follow Information Security Plan and other policies of the organization. Maintain and transmit employment records. Keep financial records, prepare financial reports. Responsible for completing the annual PCI DSS Questionnaire, maintaining records and security over credit card transactions

Computer Committee Chair: Regularly review and update this Information

IT Consultant: Install and repair computers and software. Consult on issues relating to computers or security.

CPA Firm: Audit financial records and advise on financial issues.

ACP President & Trustees: Advise in business matters.

Legal Counsel: Advise and represent in legal matters.

Appendix: Applicable Federal Regulations & Criteria

None