CSAC

CALIFORNIA
STUDENT AID
COMMISSION

CALIFORNIA STUDENT AID COMMISSION

IPA Compliant WebGrants Information Security Principles

Training Compliance to Article VI of the IPA effective July 1, 2011

CALIFORNIA STUDENT AID COMMISSION

This CSAC Info Security Training

- Satisfies requirements within IPA for CSAC supplied Information Security Training and IPA Awareness
- Increases Information Security Awareness, and
- Is required prior to WebGrants account creation or annual renewal.

CALIFORNIA STUDENT AID COMMISSION

Purpose of the IPA (Institutional Participation Agreement)

- Establish legally compliant criteria for Cal Grant eligibility.
- Establish consistent management of funds to postsecondary educational institutions and students.
- Ensure adequate security of information used in Cal Grants program.
- Non-compliance carries legal risks.

CALIFORNIA STUDENT AID COMMISSION

IPA Article VI – Info Security

- Why this Component is added
  - Financial aid & educational institutions are being targeted for fresh credit records.
  - CSAC internal risk assessment & external institution audits show high risk activity, lack of consistent security practices.
  - Requires visibility brought to executive level.
  - Increasing Legal requirements (GLBA, Civil Code 1798, CA Constitution, FERPA, etc).

CALIFORNIA STUDENT AID COMMISSION

IPA Article VI – Info Security Part 2

- Main Institutional Components
  - Top Goal – Protect Student Records
    - Legal – Why we need to do this
    - Roles/responsibilities of AO's and SA's
    - Training on privacy, security practices
    - Account mgmt & record keeping
    - Control, transmission, destruction of data
    - Notification of unauthorized access to data
    - Most requirements come from existing WebGrants Information Security and Confidentiality Agreement

CALIFORNIA STUDENT AID COMMISSION

Legal Background

- Post-Secondary Educational Institutions have been defined as Financial Institutions with the “Safeguard Rule” in 2003.
- Institutions and the CA Student Aid Commission (CSAC) are subject to State and Federal laws, including those governing Educational and Financial Institutions.

CALIFORNIA STUDENT AID COMMISSION

Security & Possession of Data

- As a result, CSAC is obligated to ensure that contractors (Institutions) adhere to security standards for its data or remove access to it.
- Institutions have the same responsibility for their data (and CSAC's data) if they contract relevant services out.
- Commission data and network access are conducted from secured onsite within the Institution (using the approved IP Address).

CALIFORNIA STUDENT AID COMMISSION

Laws Governing Institutions

- These are only SOME of the laws
  - FERPA (1972) (Family Educational Rights and Privacy Act)
  - California Constitution Article 1, Section 1 (Right to Privacy)
  - California Penal Code 502 (re: Unlawful access to data/equipment)
  - California Civil Code 1798, et seq (Information Practices Act, SSN Privacy Act, Breach Notification Act)
  - GLBA (Gramm-Leach-Bliley Act (1999), Amended in 2000 “Privacy Rule” and 2003 “Safeguard Rule”)
  - FACTA (Fair and Accurate Credit Transaction Act of 2003 - aka “Disposal Rule”)
  - SOPIPA (2016) (California’s additional constraints to federal FERPA law)

CALIFORNIA STUDENT AID COMMISSION

GLBA – A Federal Law

- Gramm-Leach-Bliley Act (GLBA)
- GLBA (1999) – Definitions, Requirements
  - Set security standards for financial institutions.
  - Defined NPI - Non-public Personal Information as ANY information in connection with providing a financial product or service to an individual unless otherwise publicly available.
    - Includes name, SSN, address, phone number, prior address, acct #, etc.

CALIFORNIA STUDENT AID COMMISSION

GLBA – Amended 2000

- GLBA (2000) – aka “Privacy Rule”
  - Defined what institutions were subject to law.
  - Educational Institutions were defined as “financial institutions”, and exemption from this law was granted citing FERPA requirements already in place.
  - But…

CALIFORNIA STUDENT AID COMMISSION

GLBA – Amended 2003

- GLBA (2003) – aka “Safeguards Rule”
  - Educational Institutions lost exemption from 2000 Privacy Rule in 2003.
  - Covers the safeguarding of information.
  - Legal interpretation by NACUA (National Association of College and University Attorneys) says…

CALIFORNIA STUDENT AID COMMISSION

NACUA Interprets “Safeguard Rule”

- Although colleges and universities are not perceived as “financial institutions” in the traditional sense (nor students or others as "customers"), the definition of that term under the GLBA regulations has brought a wide range of entities, including colleges and universities, under the jurisdiction of the GLBA Safeguards Rule.
- To add the confusion, while educational institutions that are in compliance with FERPA are generally exempt from the FTC’s GLBA Privacy Rule, there is no similar exemption afforded educational institutions under the FTC’s Safeguards Rule.

CALIFORNIA STUDENT AID COMMISSION

NACUA Interprets “Safeguards Rule”

- As a result, colleges and universities that engage in covered activities are required to develop a written information security program, and to otherwise come into compliance with the Safeguards Rule as described in this summary, by the May 23, 2003 deadline established by the FTC. Thereafter, institutions will need to follow through on the obligations undertaken in their policies by regularly testing or monitoring the information safeguards they have established.

http://www.nacua.org/nacualert/docs/GLB_Note_051603i.htm l#FN2

CALIFORNIA STUDENT AID COMMISSION

“Disposal Rule”

- Fair and Accurate Credit Transaction Act of 2003 (FACTA)
- Specific language regarding disposal of any records pertaining to ALL financial transactions - no exclusions exist for “failed transactions”.
- Disposal covers ALL avenues of release, incl. transfer, donation, sale, destruction, etc.
- Institution holding records is responsible for secure disposal of records.
- FACTA does NOT supersede record retention laws.

CALIFORNIA STUDENT AID COMMISSION

Breach Notification Law

- California SB 1386 (Civil Code 1798.29 and 1798.82) effective July 1, 2003.
- All agencies or businesses having experienced an unauthorized disclosure of unencrypted data (electronic or otherwise) of CA residents must notify ALL possibly affected individuals and data owners in a timely manner.
- Currently limited to Name and any ONE or more of the following: SSN, Passport or Drivers License #, financial acct and access #, Vehicle License Plate #.

CALIFORNIA STUDENT AID COMMISSION

Other Legal Definitions

- PII – Personally Identifying Information
  - (Nearly identical to NPI– ANY information that can be used to UNIQUELY identify an individual and can include UNIQUE descriptions).
- Breach – ANY unauthorized access to information or systems containing PII or NPI, etc.

CALIFORNIA STUDENT AID COMMISSION

Changing Legal Environment

- New laws created annually from fed/state govt.
- Responsibility for data extends to destruction. Ensure data CANNOT be restored, re-constituted, reassembled, etc.
- “E-Discovery” enacted Dec. 1, 2006 dramatically opens access to data in discovery phase of lawsuits at defendants cost. Cannot delete data believed to be subject of any possible litigation.
  - New law, with considerable confusion-to be resolved over time – However compliance is expected by Dec 2007.

CALIFORNIA STUDENT AID COMMISSION

Confused?

- Some laws define “Confidential data” or “breach” more broadly than SB1386 (California’s Breach Notification Law).
- Numerous terms used
  - NPI (Non-public Personal Information),
  - PII (Personally Identifying Information),
  - Confidential
- To be safe, don’t release ANY info, unless allowed or required by law.

CALIFORNIA STUDENT AID COMMISSION

Institution's Responsibilities

- Institution must comply with all applicable federal, California and local information security, confidentiality and privacy laws and regulations, Commission policies and requirements on data access, handling, destruction, etc.
- Institutions or staff members may lose access to WebGrants data due to lack of adherence to applicable laws and regulations.

CALIFORNIA STUDENT AID COMMISSION

Record Keeping and Titles

- The Institution must maintain 3 years of records identifying Institution Employees or its agents who are given access to GDS WebGrants.
- Do not track WebGrants for Students access.

CALIFORNIA STUDENT AID COMMISSION

Roles/Responsibilities

- Each institution's Financial Aid Director appoints a SINGLE individual as the AO (Authorized Official) that ONLY determines 1-2 SAs (System Administrators).
  - The Authorized Official has NO other WebGrants administrative duties.
- AO/SAs must sign confidentiality agreements and complete initial/annual Information Security training (this document)
- Any change in AOs or SAs requires NEW confidentiality agreements.
- AO's & SA's at additional campus locations require their own confidentiality agreements.
  - (All originals of the Confidentiality Agreements are sent to the Commission and copies kept locally for 3 years)

CALIFORNIA STUDENT AID COMMISSION

SA's Roles/Responsibilities

- SA Creates/Disables WebGrants access for applicable Institution Employees.
- SA must immediately disable username and password of institution employee(s) or agent(s) whose employment status or duties no longer require access to WebGrants.
  - (Must keep copies of documentation of this at the institution for 3 years.)

CALIFORNIA STUDENT AID COMMISSION

Required for Access to WebGrants

- SA's ensure all Institution employees or agents requiring WebGrants access sign a NEW Grant Delivery System (GDS) WebGrants User Access Request Form.
  - Used to collect all required information for security purposes.
    - No SSN's anymore.
    - Includes Last Name, First Name, Middle initial, email address, phone number.
    - Special Identifier, which will be used by the Help Desk to verify the identification of the person needing access. It can be your pet's name, your favorite food or the Model of your first car.
    - (Originals must be kept on file at the Institution)
- SA's ensure Institution employees and agents are given new/annual training on information security, privacy and confidentiality of WebGrants data.

CALIFORNIA STUDENT AID COMMISSION

SA/User Accounts

- Passwords and user identification numbers are treated as confidential and not shared.
- Passwords are changed every 90 days.
- Accounts will expire annually or unless otherwise restricted. Advanced notices of annual expirations begin 30 days prior.
- Creation/Renewal of account requires acknowledgement of employee training in privacy, information security and confidentiality.
- Individual accounts shall be disabled immediately upon termination or when their job no longer requires access to WebGrants

CALIFORNIA STUDENT AID COMMISSION

Commission Data

- All Commission data containing non-public, personally identifiable information is classified as Confidential, and should be protected appropriately.
- Institution ensures (to the best of it's ability) the accuracy, quality and completeness of data sent to the Commission.
- All Commission data no longer:
  - Required by the Institution,
  - Subject to compliance audits by the Commission, or
  - Required under record retention regulations
  - Shall be destroyed in a secure manner, regardless of media. (FACTA)

CALIFORNIA STUDENT AID COMMISSION

Security and Policies

- Institution must establish training programs and acceptable use policies for:
  - Institution employees in areas of Information Security, Privacy and Confidentiality to include Commission data.
    - (This presentation satisfies requirements for annual InfoSec training for the security of CSAC's systems/data)
- Encrypted email/physical media sent containing confidential Commission or student data. Decryption keys sent via a different method.
- Use of CSAC Student ID's should be used instead of SSN's whenever possible during correspondence with CSAC.

CALIFORNIA STUDENT AID COMMISSION

Protecting Data in Transit

- Confidential data cannot be sent via unsecured channels or media.
- Includes email, fax, CDROM, paper, magnetic media (i.e., floppy, disk, tape), USB/flash memory devices, etc.
- Use encryption or encrypted communication channels.

CALIFORNIA STUDENT AID COMMISSION

WebGrants Secure Transfer

- WebGrants now has a secure data transfer capability built in with normal WebGrants account access!
  - Upload via Data Transfer->File Upload->Secure File Transfer
  - Download via Data Transfer->Report Download->Secure File Transfer
    - Documents for download are seen only when they are available.
- Non-WebGrants users shall send encrypted files via email or physical media.

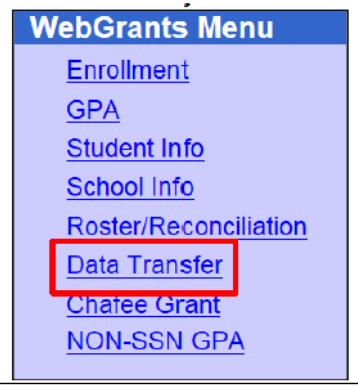
CALIFORNIA STUDENT AID COMMISSION

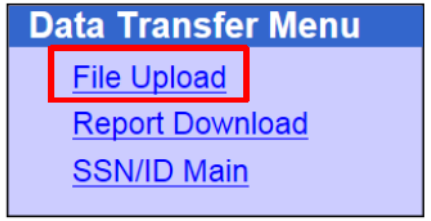
WebGrants Secure Transfer Part 2

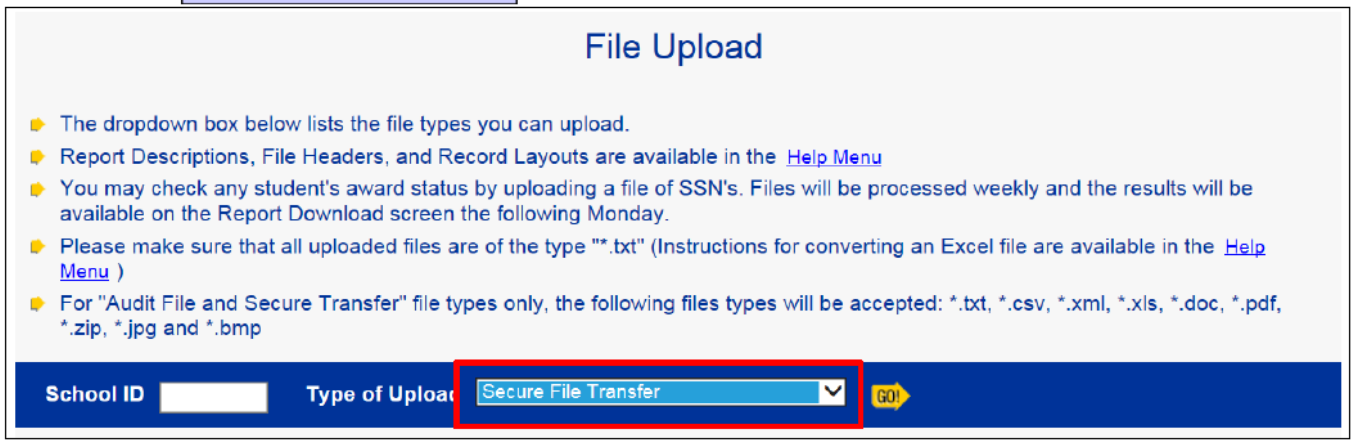
- Benefits
  - Files securely transferred online between CSAC and your school!
    - (Contact the proper CSAC department if they're not expecting the data transfer.)
- No additional need to encrypt data and send it via email or post office!
- Schools can only see their data, not shared between schools.
- No encryption passwords to remember.
- No new software to buy or install.

CALIFORNIA STUDENT AID COMMISSION

WebGrants Secure Transfer Images







CALIFORNIA STUDENT AID COMMISSION

Non WebGrants Access

- Confidential data should be sent via encrypted email or physical media.

CALIFORNIA STUDENT AID COMMISSION

Security and Policies

- Use secured systems on campus for access to WebGrants, or
- Require institution owned and managed encrypted hard drives, network connections and storage devices for off-campus access to WebGrants data.
  - Cached or saved web/Commission data can be seen/stolen from offsite personal computers in cached files, or storage devices.
  - In 2006, US Veterans Administration data stolen from contractor's home and also numerous times from unsecured office systems, affecting millions.

CALIFORNIA STUDENT AID COMMISSION

Control & Exposure of Data

- No Commission data or assets transferred to 3rd party without express written permission of the Commission's Information Security Officer (ISO).
- Institution immediately notifies the Commission of any unauthorized exposure of Commission data, followed by a report signed by the AO (Authorized Official) and Institution's Chief Executive Officer, sent within 10 business days to the Commission's ISO.
- Liability for exposure placed upon Institution through negligence of, or intentional misconduct by the Institution or its employees/agents for data in its possession.

CALIFORNIA STUDENT AID COMMISSION

Other InfoSec Practices

- Other common practices to consider…

CALIFORNIA STUDENT AID COMMISSION

Other InfoSec Practices Part 2

- Systems infected with “key loggers” or “spyware” can grab usernames & passwords used to log in to WebGrants
  - Consider this risk for offsite or onsite system security.
  - WebGrants logins & activity logged at CSAC.
- Securely retrieve, store and/or destroy all printouts/reports containing Confidential information.
- Institutions network and system must be secured with virus protection and firewall protection.

CALIFORNIA STUDENT AID COMMISSION

Other InfoSec Practices Part 3

- Screen lock should be used when your computer is unattended.
  - “CTRL-ALT-DEL when you leave your seat”
- Adopt a “Clean-desk policy” for secure work areas to eliminate improper exposure of Confidential data.
- Hard drives must be sanitized before re-use, repair, disposal or sale. Deleted data can be recovered easily.
  - Encrypted hard drives avoid this problem.
  - Offsite tech support can expose data.
  - Formatting a drive does not sanitize the disk!

CALIFORNIA STUDENT AID COMMISSION

Other InfoSec Practices Part 4

- Don’t discuss Confidential data openly or loudly for others to overhear.
- Know what Confidential data is and where it’s located.
  - Don’t email unencrypted Confidential information.
  - Don’t take it home or leave in unsecured locations.
  - Pick up printouts immediately after printing.
  - Confidential information has very real value for scammers.

CALIFORNIA STUDENT AID COMMISSION

Other InfoSec Practices Part 5

- Ensure that requests for information come from real and legitimate individuals or legal channels.
  - Social-Engineering (in-person, via phone or email) is a common tactic to request information by pretending to be someone they're not.
- Lock down machines to prevent Administrator access rights.
  - Greatly reduces ability for malicious software to be installed without user knowledge.

CALIFORNIA STUDENT AID COMMISSION

Other InfoSec Practices Part 6

- Secure your web site, kiosks, networks and databases by keeping current on patches.
  - New levels of attacks occurring more rapidly
    - Databases attacked via web page coding.
    - Web pages being hacked.
    - Browsers being attacked while browsing.
    - Networks and VOIP (Voice over IP phones) can be sniffed for data.
    - Applications (web, graphics, office software) can be vulnerable. \
    - Secure kiosks & network wiring to prevent access to data.
    - Lock down access to data on a “need-to-know” basis.

CALIFORNIA STUDENT AID COMMISSION

Other InfoSec Practices Part 7

- Observe WebGrants failed login information to detect attempts by others to use your account.
- Log out of your WebGrants sessions when finished.
- Don’t share your WebGrants password or User ID.

CALIFORNIA STUDENT AID COMMISSION

Other InfoSec Practices Part 8

- Eliminate or minimize use of insecure wireless connections for Confidential work.
  - Unencrypted traffic easily stolen.
  - WEP security broken within seconds.
  - WPA security can be broken over time.
  - WPA2 can be hacked very easily by a professional. No wireless should be considered secure.
  - Bluetooth can be hacked easily, even for many PDA's/phones with "Discover Mode" turned off.
  - PDA's, smart phones & Blackberries are potential avenues for data to be lost, stolen or leaked.

CALIFORNIA STUDENT AID COMMISSION

Other InfoSec Practices Part 9

- Eliminate the ability for USB memory devices and music players to connect to machines.
  - They can run or spread malicious programs
  - They can snoop your system/network
  - They can steal/download your data
  - They can disable anti-virus programs
  - They can open back-door channels for attacks or sending out information
  - All this can be done silently, and undetectably!

CALIFORNIA STUDENT AID COMMISSION

Other InfoSec Practices Part 10

- Provide an InfoSec Awareness campaign with annual training and regular reminders.
  - Make training sensible and realistic
  - Implement & Support Infosec policies
  - Train employees on InfoSec Policies/practices
  - Humans are often the weakest link.

CALIFORNIA STUDENT AID COMMISSION

Why Information Security?

- Colleges and financial institutions are targeted for the Confidential information on new students having fresh credit histories.
- Alumni, donors, applicants and past/present employee records can be targeted.
- The information gained can be used elsewhere.
- Steep financial cost and loss of confidence to the institution.

CALIFORNIA STUDENT AID COMMISSION

Why Information Security Part 2?

- Colleges and financial institutions are targeted for the Confidential information on new students having fresh credit histories.
- Alumni, donors, applicants and past/present employee records can be targeted.
- The information gained can be used elsewhere.
- Steep financial cost and loss of confidence to the institution.

CALIFORNIA STUDENT AID COMMISSION

Contact Information

- For questions and assistance in completing the form contact:
  - Institutional Support (888) 294-0153
- For WebGrants assistance with Password Resets contact:
  - IT Service Desk (888) 294-0148
- To report potential security issues: **iso@csac.ca.gov**
- **Send completed forms: webgrantsaccess@csac.ca.gov**