

IPA Compliant WebGrants Information Security Principles

Training for Compliance to Article VI of
the Student Aid Commission IPA
effective July 1, 2007



This CSAC InfoSecurity 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.



Purpose of IPA

(Institutional Participation Agreement)

- Establish legally compliant criteria for CalGrant eligibility.
- Establish consistent management of funds to post-secondary educational institutions and students.
- Ensure adequate security of information used in CalGrants program.

- Non-compliance carries legal risks



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)



IPA Article VI - Info Security

■ 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**



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.



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.



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")



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, address, acct #, etc.



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....



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....



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 to 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.

(cont on next slide)



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.html#FN2



“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.**



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 + (SSN or Drivers License # or any financial acct/access #)



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.



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.



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.



That's it for the legal stuff...

Now...

On to the IPA Security Requirements...



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.



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.



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)



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.)



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 or Mother's maiden name anymore.
 - Includes email address, other contact info.

(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.



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 should be disabled immediately upon termination or when their job no longer requires access to WebGrants.



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)



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)**
 - No faxes or unencrypted 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.**



Protecting Data in Transit

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



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 should send **encrypted** files via email or physical media.



WebGrants Secure Data Transfer

■ 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!



WebGrants Secure Data Upload

- [Roster/Reconciliation](#)
- [Data Transfer](#)
- [Chafee Grant](#)

Data Transfer

- [File Upload](#)
- [Report Download](#)
- [SSN/ID Main](#)
- [Report Notification Prefs](#)

File Upload

- The dropdown box below lists the file types you can upload.
- Report Descriptions, File Headers, and Record Layouts are available in the [Help Menu](#)
- You may check any student's award status by uploading a file of SSN's. Files will be processed weekly Report Download screen the following Monday.
- Please make sure that all uploaded files are of the type "*.txt" (Instructions for converting an Excel file a
- For "Audit File and Secure Transfer" file types only, the following file types will be accepted: *.txt, *.c

School ID = Type of Upload

Browse and select files to upload		
1	<input type="text"/>	<input type="button" value="Browse..."/>
2	<input type="text"/>	<input type="button" value="Browse..."/>
3	<input type="text"/>	<input type="button" value="Browse..."/>
4	<input type="text"/>	<input type="button" value="Browse..."/>



WebGrants Secure Data Download

- [Roster/Reconciliation](#)
- [Data Transfer](#)
- [Chafee Grant](#)

Data Transfer

- [File Upload](#)
- [Report Download](#)
- [SSN/ID Main](#)
- [Report Notification Prefs](#)

Report Download for UNIV OF CA -

- To download or display a report or data file click on the Retrieve File button.
- All data columns can be sorted either ascending or descending order by clicking on the blue column headings.
- To compare two roster files, select Grant Roster for Report and Data File for Media Type.
- To delete uploaded Audit Files, select Audit File for Report and the Delete checkbox column will appear.

School ID = Acad Year = Month =
 Report = Media Type = GO! ➤

Report Date	Description	Media Type	Month	Delete	
29-MAY-08	Secure File Transfer / New Text Document.txt (05-29-08 02:12 PM)	Data File	MAY	<input type="checkbox"/>	Retrieve File
29-MAY-08	Secure File Transfer / dilbert21466360070521.gif (05-29-08 02:12 PM)	Data File	MAY	<input type="checkbox"/>	Retrieve File

Delete File



Non WebGrants access

- Confidential data should be sent via encrypted email or physical media – instructions seen in following pages



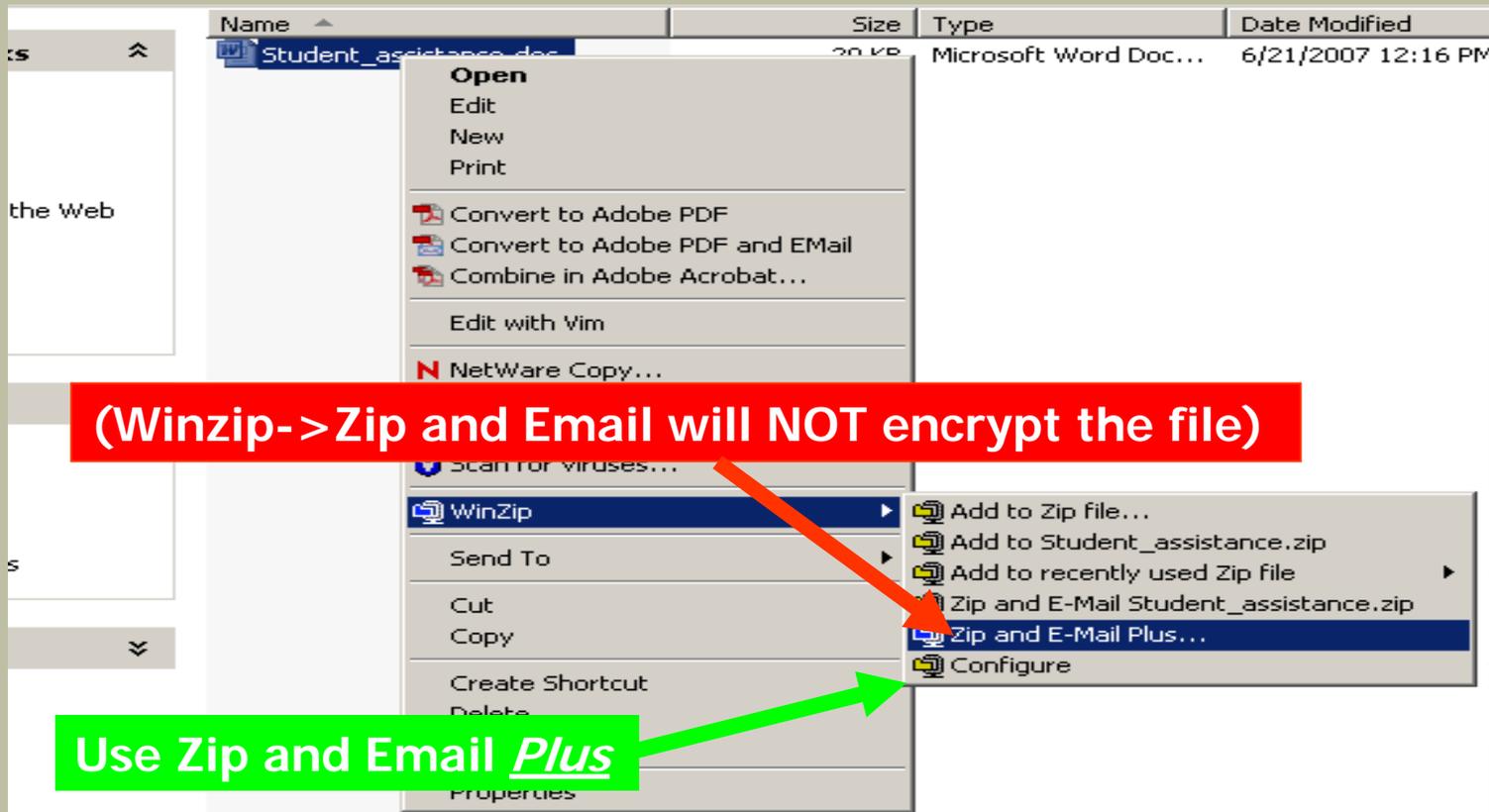
Encryption tools

- WinZip - <http://www.winzip.com>
 - Free during evaluation period, requires payment after eval period.
 - Compresses most files, encrypts
- 7Zip - <http://www.7-zip.org>
 - Free, no license restrictions
 - Compatible w/WinZip and many other archive tools, encrypts
 - Use ZIP-AES-256 encryption



Encrypting Confidential Data & Mailing It Securely - WinZip

- Right click on file(s) to be encrypted/sent
- Select WinZip->Zip and Email **Plus** (only!)



Encrypting Confidential Data & Mailing It Securely – WinZip (cont)

- Turn on the Encryption option, press OK
- Enter the same password in each field
- Select 256-Bit AES Encryption.
- Press OK



Encrypted Email send

- Email windows appears with **encrypted** document(s) attached.
- Do NOT send the password with the attachment – call recipient or send it in a separate email.



Encrypting with older versions or other software

- Establish a new Zip archive in a desired directory. Name the file with the student's CSAC ID & date (ie, 1234567_20070621.zip)
- Specify that you want the zipped file to be encrypted.
 - Use STRONG encryption (ie, AES) - Some are very weak.
- Add files to the archive (may be asked to encrypt them at this time)
- Save and close the archive. Test it by double-clicking it, and ensuring that it requests a decryption password.
- Open a new email
- Attach the Encrypted, zipped file, add a message, then send it off.
Do not include the password in the message – send it separately in a new message or call the recipient.
- Ensure arrival of the file, as some filters block zip files.



Secure FAX

- At this time, there is no good solution to send an encrypted fax
 - Too many standards – not all machines set up to txfer/receive encrypted faxes.
- Instead, Scan your document to a file, then encrypt it and send via email, or
- Redact all Confidential information before faxing.
- Alternative – call recipient before faxing to let them know it is coming, and to verify the fax number.
- Don't let fax sit unattended.



Security and Policies

- Use secured systems on campus for access to WebGrants, or
- Require 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.



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 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.



Other InfoSec Practices

- Other common practices to consider....



Other InfoSec Practices

- Systems infected with “keyloggers” 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.



Other InfoSec Practices

- 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!



Other InfoSec Practices

- 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



Other InfoSec Practices

- 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.



Other InfoSec Practices

- 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.



Other InfoSec Practices

- Flush web browser cache regularly, to eliminate stored WebGrants reports & data
 - Internet Explorer:
 - Tools->Internet Options->General->Temporary Internet Files
 - Mozilla Firefox:
 - Tools->Options->Privacy->Privacy Options



Other InfoSec Practices

- 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.



Other InfoSec Practices

- 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 is being targeted for cracking
 - 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.



Other InfoSec Practices

- 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!



Other InfoSec Practices

- 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.



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.



Questions? Suggestions?

Contact Info

- Contact the CSAC Helpdesk at
 - 1-888-294-0148

- CSAC Information Security Officer
 - California Student Aid Commission
 - PO Box 419026
 - Rancho Cordova, CA 95741-9026
 - iso@csac.ca.gov

