Original version:10.04.2021
Updated version: 10.04.2021
Executed Version: 10.04.2021

Standards for Safeguarding Customer Information
Policy and Procedures

Upon signing a Program Participation Agreement (PPA), DSDT agreed to comply with the Family Educational Rights and Privacy Act (FERPA), the U.S. Department of Education's implementing regulations at 34 C.F. R. Part 99, and the Standards for Safeguarding Customer Information, 16 C.F.R. Part 314, issued by the Federal Trade Commission (FTC), as required by the Gramm-Leach-Bliley (GLB) Act, P.L. 106-102. DSDT is responsible for complying with the limitations on the disclosure of PII in students' education records under FERPA and is subject to Sections 501 and 505(b)(2) of the GLB Act.

The GLB Act, also known as the Financial Services Modernization Act of 1999 (Public Law # 106-102, 113 Statute 1338), regulates the collection, disclosure, and protection of consumers' nonpublic personal information or personally identifiable information (PII) by financial institutions. Section 501 of GLB Act established the following information security standards for financial institutions:

DSDT shall establish appropriated standards for DSDT relating to administrative, technical, and physical safeguards-

(1) To ensure the security and confidentiality of students and employees records and information
(2) To protect against any anticipated threats or hazards to the security or integrity of such records; and
(3) To protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any student or employee.

Program Objectives:

The objectives of this Information Security Program ("Program") are as follows:

- Ensure the security and confidentiality of DSDT students' and employee's information.
- Protect against any anticipated threats or hazards to the security and/or integrity of the institution's Student's and employee's information.
- Protect against unauthorized access to or use of the Institution's students and employee's information that could result in substantial harm or inconvenience to any customer.

Statement of Purpose

The plan is to protect the alteration or destruction or other compromise and is in place to execute the safeguards in place minimizing and negating the risks in the following operations within our organization including:

Responsibilities: DSDT has implemented reasonable expectations that are readily accessible and are designed to achieve the objectives mentioned above. The persons within DSDT responsible for the information security program are management and the Information Technology Lead (ITL) within our organization. The ITL manages the majority of the operations in regard to the internal and external risks that may compromise the security and confidentiality of customer information. The ITL at DSDT, designs, manages and implements information safeguards ultimately controlling the risks to our organization. The way this is done is through regularly testing or otherwise monitoring the effectiveness of our safeguarding procedures within our control systems. The ITL at DSDT will also ensure the oversight of all other service providers contracted or hired, by maintaining and retaining only qualified individuals or companies capable of safeguarding customer information. The ITL at DSDT will evaluate on a quarterly basis and adjust DSDT's information security program as needed in lieu of test results from the continual monitoring of safeguards. In the event we believe we may have a material impact on any information whether digital or print, we will alter our plan to accommodate. Any breaches of this

program must be reported immediately to the School's Director or Chief Operations Officer at 313-263-4200, in order to assess the potential damage such breach may impose on our affected customer. Steps will be taken to re-secure information and any affected systems will be examined to ensure future compliance. In the event the Information Technology Lead or the direct management leaves the employment of the Institution, the School Director or Chief of Operations, shall take over the responsibilities of the Information Technology Lead, until a new Technology Lead is designated.

Procedures

1. All records containing customer information shall be stored and maintained in a secure area.
    - Paper records are stored in a fire-proof safe, in a locked room, that is locked when unattended. The School Director/ Chief of Operations and ITL control access to such areas.
    - All storage areas are protected against destruction or potential damage from physical hazards, like fire or floods and are kept in fire-proof safes.
    - Electronic customer information is stored on secure servers. Access to such information is password controlled, and the ITL shall controls access to the internal servers.
    - Student and employee information consisting of financial or other similar information (e.g., social security numbers, etc.) are not be stored on any computer system with a direct Internet connection.
    - All customer information is backed up on a [daily] basis. Such back up data is stored in a secure location as determined by the ITL.

2. All electronic transmissions of student and employee information, whether inbound or outbound, are performed on a secure basis.
    - Social Security, IRS information, or other sensitive financial data transmitted to DSDT directly from students shall use a secure connection, such as a Secure Sockets Layer (SSL) or other currently accepted standard, so that the security of such information is protected in transit. Such secure transmissions are automatic. Students are advised against transmitting sensitive data, like social security, via electronic mail.
    - DSDT requires by contract that inbound transmissions of student information delivered to DSDT via other sources be encrypted or otherwise secured.
    - All outbound transmissions of student information is secured in a manner acceptable to the ITA.
    - To the extent sensitive data must be transmitted to DSDT by electronic mail, such transmissions are password controlled or otherwise protected from theft or unauthorized access at the discretion of the ITA.
    - The ITA and third-party service reviews all students' applications to ensure an appropriate level of security both within DSDT and with the Institution's business third party server and IRS.

3. All paper transmissions of customer information by DSDT are performed on a secure basis.
    - Sensitive student information is always properly secured.
    - Student information delivered by DSDT to third parties is always kept sealed.
    - Paper-based student information is never left unattended in an unsecured area.

4. All student information is disposed of in a secure manner.
    - The ITA supervises the disposal of all records containing student information.
    - Paper based student information is shredded and stored in a secure area until a disposal or recycling service picks it up.

- All hard drives, diskette, magnetic tapes, or any other electronic media containing student information shall be erased and/or destroyed prior to disposing of computers or other hardware. All hardware is effectively destroyed.
- All student information is disposed of in a secure manner after any applicable retention period.

5. The ITA maintains an inventory of Institution computers, including any handheld devices or PDAs, on or through which student information may be stored, accessed or transmitted.

6. The ITA develops and maintain appropriate oversight or audit procedures to detect the improper disclosure or theft of student information.

Definitions

As used in the Gramm-Leach-Bliley Act, "customers" include those to whom DSDT provides financial services of any kind. For the purposes of this Safeguarding Program, "customer information" is defined as any record containing non-public, personally identifiable financial information regarding any of the School's customers, whether such records are maintained on paper, electronically or by any other means, this Security Program, in and of itself, does not create a contract between the student and any person or entity

Applicability

This Information Security Program applies to all DSDT departments with access to student loan data or other customer information regardless of the purpose or frequency of use and applies to the gathering, storing, processing, transmitting and disposing of customer information. This Program also applies to outside service providers, such as loan servicing agents and collection agencies to which student loan data may be transferred or who may gather it on behalf of the School.

Information Security Policies and Procedures

Detecting, Preventing and Responding to Attacks, Intrusions or Other Systems Failures In keeping with the objectives of the Program, DSDT implements, maintain and enforce the following attack and intrusion safeguards:
Campus Café, DSDT's educational management software.
Boston Educational Network, a school interface that is encrypted. The school must be secured with a unique logon ID and password for access to systems.

1) The ITA ensures DSDT has adequate procedures to address any breaches of the Institution's information safeguards that would materially impact the confidentiality and security of customer information. The procedures shall address the appropriate response to specific types of breaches, including hackers, general security compromises, denial of access to databases and computer systems, etc.
2) The ITA utilizes and maintains a working knowledge of widely available technology for the protection of student information.
3) The ITA communicates with the Institution's computer vendors from time to time to ensure that DSDT has installed the most recent patches that resolve software vulnerabilities.
4) DSDT utilizes anti-virus software that updates automatically.
5) DSDT maintains up-to-date firewalls.

6) The ITA manages the Institution's information security tools for employees and pass along updates about any security risks or breaches.
7) The ITA establishes procedures to preserve the security, confidentiality and integrity of student information in the event of a computer or other technological failure.
8) The ITA ensures that access to student information is granted only to legitimate and valid users.
9) The ITA notifies students promptly if their student information is subject to loss, damage or unauthorized access.

Information Technology Lead

DSDT has implemented reasonable expectations that are readily accessible and are designed to achieve the objectives mentioned above. The persons within DSDT responsible for the

The plan is to protect the alteration or destruction or other compromise and is in place to execute the safeguards in place minimizing and negating the risks in the following operations within our organization including:

1. Employee Training and Management
2. Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
3. Detecting, preventing and responding to attacks, intrusions, or other systems failures.

The ITL at DSDT, designs, manages and implements information safeguards ultimately controlling the risks to our organization. The way this is done is through regularly testing or otherwise monitoring the effectiveness of our safeguarding procedures within our control systems. The ITL at DSDT will also ensure the oversight of all other service providers contracted or hired, by maintaining and retaining only qualified individuals or companies capable of safeguarding customer information.

The ITL at DSDT will evaluate on a quarterly basis and adjust DSDT's information security program as needed in lieu of test results from the continual monitoring of safeguards. In the event we believe we may have a material impact on any information whether digital or print, we will alter our plan to accommodate.

Compliance Procedures

In each affected area, the ITL will identify and assess all levels of risk to DSDT customers and implement the following procedures to ensure compliance. It is the responsibility of the ITL to evaluate and assess the risks of any changes made with regard to services offered, implementation of new procedures, policies or services and to make the necessary changes and/or adjustments to ensure continued compliance.

Within each area, the ITL will regularly monitor and test this Program to ensure compliance and make all necessary changes as required by the results of such testing and monitoring. Employees will remove customer information from desktops and any areas of public access such as counters, the top of file cabinets, tables, printers, copiers and FAX machines. Offices containing customer information will be locked at night and access to offices engaged in the provision of financial services such as Student Loans, Collections, Student Accounting Services and Financial Assistance will be restricted to authorized personnel only. All promissory notes will be stored in

locked, fireproof file cabinets in restricted-access, locked storage rooms where Student Loan files are stored.

With respect to electronic data, customer information shall be protected by this Information Security Program, including provisions regarding password confidentiality, the periodic changing of passwords, restriction of access to personal computers and elimination of storage of customer information on generally accessible machines. Care will be taken to ensure the protection of all information disseminated by FAX, data transferred electronically, and data stored online.

The Family Educational Rights and Privacy Act (FERPA), the Fair Debt Collection Practices Act (FDCPA) and other laws governing the dissemination of information to third parties will be appropriately enforced. Designated personnel will monitor compliance, evaluate the effectiveness of this Information Security Program and collaborate with other DSDT officials in implementing any needed adjustments to this Program. Outside service providers will be required by contract to implement and monitor safeguards sufficient to protect customer information as required by the Gramm-Leach-Bliley Act. The sale, lease, license or other distribution of customer information, including lists, abstracts and summaries of any kind is strictly prohibited.

Disposal

DSDT requires the shredding of all paper containing any customer information prior to disposal. In the event of any recycling of personal computers containing customer information, all memory components of such computers will be completely reformatted or otherwise erased for any new use as determined by the department.

System Failures

In order to prevent breaches of this Program, assigned personnel will test data security systems governed by this Program for weaknesses, monitor performance of service providers and conduct physical security analyses of both electronic and hardcopy records. This will ensure that all Program goals are being met and that DSDT customers can be secure in the knowledge that their personal financial information is protected.

Any breaches of this program must be reported immediately to the School's Director or Chief Operations Officer at 313-263-4200, in order to assess the potential damage such breach may impose on our affected customer. Steps will be taken to re-secure information and any affected systems will be examined to ensure future compliance.

Questions

Questions regarding the Gramm-Leach-Bliley Act, the Fair Debt Collection Act and Family Educational Rights and Privacy Act should be referred to the Director of Admissions at 313-263-4200.

Questions regarding the DSDT Information Security Policy should be referred to the Information Technology Lead at 313-263-4200.

Frequently Asked Questions about Cybersecurity Compliance

Who needs to worry about data security?
Data security affects everyone at a postsecondary institution (PSI) from the president to applicants. No one is exempt from data security, and each person has a role in ensuring data security.

Why do I need to worry about data security?
You should worry about data security for three reasons. First, the educational sector has an initial level of security maturity, as assessed by Gartner, which results in high risk and low cybersecurity maturity. Second, the educational sector is a rich trove of email addresses and credentials, financial information, research, and development. Third, PSIs that distribute Title IV funds have entered into agreements with FSA via a Program Participation Agreement (PPA) and a Student Aid Internet Gateway (SAIG) Agreement. Those agreements include stipulations about safeguarding data.

What are data security requirements?
Title IV PSIs are financial institutions per the Gramm-Leach-Bliley Act (GLBA, 2002). Per the Federal Student Aid (FSA) Program Participation Agreement (PPA) and the Student Aid Internet Gateway (SAIG) Agreement, PSIs must have GLBA safeguards in place. PSIs without GLBA safeguards may be found administratively incapable (unable to properly administer Title IV funds). GLBA safeguards require institutions to:

- develop, implement, and maintain a documented data security program;
- designate an employee or employees to coordinate the program;
- identify reasonably foreseeable internal and external risks to data security via formal, documented risk assessments of:
    - employee training and management;
    - information systems, including network and software design, as well as information processing, storage, transmission, and disposal; and
    - the ability to detect, prevent, and respond to attacks, intrusions, or other systems failures;
- control the risks identified, by designing and implement information safeguards and regularly test/monitor their effectiveness;
- oversee service providers by
    - taking reasonable steps to select and retain service providers that can maintain appropriate safeguards for the FSA, student, and school (customer) information at issue; and
    - requiring your service providers by contract to implement and maintain such safeguards; and
- evaluate and adjust your school's data security program considering
    - the results of the required testing/monitoring,
    - any material changes to your operations or business arrangements, and
    - any other circumstances that you know may have a material impact on your information security program.

Further, Title IV schools are subject to the requirements of the Federal Trade Commission Identity Theft Red Flags Rule ("Red Flags Rule") (72 Fed. Reg. 63718) issued Nov. 9, 2007. The Red Flags

Rule requires an institution to develop and implement a written identify theft prevention program to detect, prevent, and respond to patterns, practices, or specific activities that may indicate identity theft.

What is a breach?
Per GLBA, PSIs must protect against any unauthorized disclosure, misuse, alteration, destruction, or other compromise of information, such as unauthorized access. The Department of Education and Federal Student Aid considers each of these a breach. Each PSI must have in place administrative, technical, and physical safeguards which:

- ensure the security and confidentiality of customer information,
- protect against any anticipated threats or hazards to the security or integrity of such records, and
- protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

When do I report a breach?
The Student Aid Internet Gateway (SAIG) Agreement requires that as a condition of continued participation in the federal student aid programs, PSIs report actual data breaches, as well as suspected data breaches. Title IV PSIs must report on the day that a data breach is detected or even suspected. The U.S. Department of Education (the Department) has the authority to fine institutions—up to $54,789 per violation per 34 C.F.R. § 36.2—that do not comply with the requirement to self-report data breaches. The Department has reminded all institutions of this requirement through Dear Colleague Letters (GEN 15-18, GEN 16-12), electronic announcements, and the annual FSA Handbook.

How do I report a breach?
To report a breach, email cpssaig@ed.gov. Your email should include:

- date of the breach (known or suspected),
- impact of the breach (number of records, number of students, etc.), • method of the breach (hack, accidental disclosure, etc.),
- information security program point of contact (email address and phone number are required),
- remediation status (complete, in-process, etc. with detail), and
- next steps (as needed).

If you cannot email, you should call the Department's security operations center (EDSOC) at 202-245-6550 to report the data listed above. EDSOC operates 24 hours a day, seven days per week.

We recently heard in an FSA conference session that we can no longer accept faxed or emailed copies of taxes or tax transcripts. Is this the case?
Are we permitted to accept such documents via a student's school email account?
PSIs should never solicit personally identifiable information (PII)—especially sensitive personally identifiable information (SPII)—through means that are known to be insecure. PSIs should review their information requests and guidance to students and parents to ensure that instructions are clear about the explicit protection of data and how to transmit data securely transmittal.
PSIs must have secure means to receive inbound PII and SPII from students and parents. Secure means could include an appropriately safeguarded fax, a secure web portal to upload data and documents, student email accounts that encrypt communications to at least an AES-256-bit level, or separately encrypted attachments that are password protected (with the password provided in a separate email).

PSIs must remediate all data breaches. A data breach could be created if a student or parent sends PII or SPII via unsecure means, which would allow PII or SPII to be accessible by individuals who do not have a need to know.
PSIs must remediate this type of data breach immediately each time it occurs. However, at this time, this type of data breach does not need to be reported as an institutional data breach to FSA.

How can students or parents create an encrypted attachment to send to a PSI?
There are many applications that have the ability to encrypt attachments. An example is provided below for WinZip™, with the caveat that this is not the only acceptable method, and unless very carefully configured, WinZip would not fit the Federal Information Processing Standard (FIPS) which is defined by FIPS 140-2. The minimum acceptable encryption is AES 256- bit for PSIs.

WinZip instructions for file/folder encryption and password protection:
1) Open a folder to the location of the file(s)/folder(s) that you wish to encrypt.
2) Select the file(s)/folder(s) that you wish to encrypt. Note that in order to select more than one file/folder, you must press the "Ctrl" key on the keyboard while selecting them.
3) Right-click over one of the selected items.
4) Select WinZip. From the submenu that appears, select "Add to Zip File."
5) In the "Add Files" dialog box, specify a 'File name' and 'Destination' (location) for the finished Zip file.
6) Select ". Zip" as the Compression Type.
7) Under Encryption, check the "Encrypt files" box.
8) Click the "Add" button.
9) A pop-up window may appear saying "You should be aware of the advantages and disadvantages of the various encryption methods before using this feature. Please press the F1 key for more information, particularly if this is the first time you are using encryption." Select the "OK" button to continue.
10) In the "Enter Password" field, enter an appropriate password. Passwords must be at least eight characters and must contain at least one of each the following: a lowercase character (a-z), an uppercase character (A-Z), a number character (0-9), and a symbol character (!, @, #, $, %, ^, &, *, etc.).
11) In the "Re-enter Password" field, enter the same password from Step #10, and remember the password for future reference.
12) Click the "OK" button.
13) A pop-up window may appear saying "Add Complete. Your files have been added. The files will be compressed and encrypted when saved." Click the "OK" button to continue.
14) The encrypted WinZip file should be in the location identified in Step #5 above.
15) The password must not be included in the same message and should either be included in a separate email or verbally provided to the intended user.

What if we have the documents faxed? Our fax has documents going straight to the document imaging/storage area on a server. Paper does not print. Is this an acceptable practice? Can a fax in-transmission be hacked?
Faxing, if safeguarded, is not a breach. It is assumed that a PSI has already performed a risk assessment and has secured access to the physical server. It is a further assumption that technical and logical controls are in place that would prevent individuals without a need to know (for example, system Representatives) from viewing PII or SPII.
More specifically, faxes arriving securely would depend on the method of how it arrives. If the fax is printed upon arrival from a fax machine or if the fax is transmitted to a server, physical and administrative safeguards must ensure the data are only viewed or handled by authorized personnel

with a need to know. Confidentiality and integrity are each key whether it is physical or digital. The fax-hack question is substantively different. A lot would depend on if your institution is leveraging a Private Branch Exchange (PBX) or if it is a straight Signaling System 7 (SS7) connection to the standard Public Switched Telephone Network (PSTN). Physical or logical access to the PBX on your campus or cloud has the potential for breach, as well physical access to your PSTN equipment. Any of these could potentially cause a breach in the confidentiality of the data. However, as a PSI, your team should do a risk assessment of your technology design and handling process to review where risks exist and put in the appropriate controls or compensating controls. You also should document your risks and controls in your information security program document. Examples include putting the fax machine (PTSN connection, physical print-out type that is the non-networked standard) in a controlled space that only authorized personnel can access. For the hack risk, you might inspect from the demarcation point to the device regularly to ensure no interception evidence. You may further document the security controls inherited via your ILEC/CLEC (telephone service carrier). Regular testing also should be documented to show that your PSI has given this thoughtful consideration.