567 S Valley View Dr. St. George, UT 84770. 435-261-4203. www.zmc.edu

Data Protection & Security Policy

Zion Massage College is committed to ensuring that all confidential and other sensitive information is safeguarded from unauthorized access, use, modification or destruction. All members of our campus community share in the responsibility of protecting the confidentiality and security of data.

The Data Protection and Security Policy focuses on confidential and sensitive information, including Personally Identifiable Information (PII) and those data elements protected by the Family Educational Rights and Privacy Act (FERPA) as well as relevant Security Directives as issued by the ZMC Administrative team in consultation with the ZMC Program Advisory Committee.

Purpose:

The purpose of this policy is to outline essential roles and responsibilities within the ZMC community for creating and maintaining an environment that safeguards data from threats to personal, professional and institutional interest and to establish a comprehensive data security program in compliance with applicable laws and regulations.

This policy is also designed to establish processes for ensuring the security and confidentiality of confidential information and to establish administrative, technical and physical safeguards to protect against unauthorized access or use of this information.

To Whom Does This Policy Apply:

This policy applies to all ZMC faculty and staff, whether full or part-time, paid or unpaid, temporary or permanent, as well as to all other members of the ZMC community.

This policy applies to all information collected, stored or used by or on behalf of any operational unit, department and person within the community in connection with ZMC operations.

Data Classification

All information covered by this policy is to be classified into one of three categories, according to the level of security required. These categories or “security classifications” are

Confidential information:

includes sensitive personal and institutional information, and must be given the highest level of protection against unauthorized access, modification or destruction. Unauthorized access to personal Confidential information may result in a significant invasion of privacy, or may expose members of the ZMC community to financial risk. Unauthorized access or modification to institutional Confidential information may result in direct, materially negative impacts on the finances, operations or reputation of ZMc. Examples of personal Confidential information include information protected under privacy laws (including, without limitation, the Family Educational Rights and Privacy Act and if applicable, the Health Information Portability and Accountability Act), information concerning the pay and benefits of ZMC employees, personal identification information or medical/health information pertaining to members of the ZMC community. Institutional Confidential information may include College financial and planning information, legally privileged information, and other information.

Without limiting the generality of the foregoing, Confidential information shall include “personal information” as defined by RCW 42.56.100- Protection of public records - public access and RCW 42.56.420 - Security with any one or more of the following:

(a) Social security number
(b) Driver’s license number or state -issued identification number;
(c) Financial account number, or credit card or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to the resident’s financial account and confidential information also includes “customer information,” defined by the *safeguards rule* under the Gramm-Leach-Bliley Act to mean any information containing personally identifiable information that the College obtains in the process of offering a financial product or service. You can find out more about the GLBA here: https://youtu.be/06ah9arELG4

Internal Use Only information:

includes information that is less sensitive than Confidential information, but that, if exposed to unauthorized parties, may have an indirect or possible adverse impact on personal interest, or on the finances, operations, or reputation of ZMC. Examples of this type of data from an institutional perspective include internal memos meant for limited circulation, or draft documents subject to internal comment prior to public release.

Public information:

Is information that is generally available to the public, or that, if it were to become available to the public, would have no material adverse effect on individual members of the ZMC community or upon the finances, operations, or reputation of ZMC.

All Information Resources, whether physical documents, electronic databases, or other collections of information, are to be assigned to a security classification level according to the most sensitive content contained therein.

Where practicable, all data is to be explicitly classified, it is to be treated as follows; Any data that includes any personal information concerning a member of the College community (including any health information, financial information, academic evaluations, social security numbers or other personal identification information) shall be treated as Confidential. Other information is to be treated as Internal Use Only, unless such information appears in form accessible to the public (i.e., on a public website or a widely distributed publication) or is created for a public purpose.

Respecting Your Privacy and Protecting Your Personal Data

ZMC collects information to better understand the needs of our students and campus community. This information helps us improve our services and communication between students, staff and all members of the ZMC community.

ZMC conducts business in compliance with the Personal Data Protection Act (PDPA) and has implemented additional measures to protect the personal information and privacy of our students, staff members and Massage Therapy Clinic clients.

Ways that ZMC collects your personal information:

- Submit an online request for more information
- Contact us with a question or request for more information
- Apply for admission at ZMC
- Apply for employment with ZMC
- Attend a course conducted by ZMC
- Visit our website
- Participate in a survey

The information we collect:

- Your identity - This includes information from identification documents that you may submit in the admissions process or in requests for information.
- Your interaction with us - This may include information from interactions such as notes from a call that you make to us, an email or letter that you send to us or other records of any contact that you have with ZMC staff members.
- Your student account information - This includes information from your admission application, tuition ledger and other information, which is contained in your student file.

How we use your information:

We may use your information for:

- Administration of services
- Processing of your application for admission
- Enabling us to process bills and payments
- Responding to enquiries and requests from you or people you have authorised
- Informing you about Prana Experiences and other program offerings at ZMC

We may amend or modify this Polciy from time to time, such as in response to changes to legislation. We remain committed to safeguarding your information and being open about our data protection practices.

In addition to ZMC's Data Protection Policy, all ZMC students are protected by the United States Family Educational Rights and Privacy Act of 1974 (FERPA). FERPA is a federal law designed to protect the privacy of and limit access to student educational records. FERPA grants students certain rights, privileges and protections relative to the identifiable information contained within their educational records maintained by ZMC. Specifically:

- Students have some control over the disclosure of information. A student's educational records (with the exception of directory information) will be released to third parties outside of ZMC only with the written consent of the student.
- Students have the right to inspect, review and request amendment of their educational records.
- Students have the right to challenge information contained within their educational records.
- Students have the right to file a complaint with the U.S. Department of Education if they believe their rights under FERPA are violated.

Roles and Responsibilities

It is the policy of ZMC that all confidential and other sensitive information be safeguarded from unauthorized access, use, modification or destruction. All members of the ZMC community share in the responsibility for protecting the confidentiality and security of data. This section of the policy assigned specific duties to each of the roles of Designated Information Security Officer, Program Director, Data Stewards and Users:

Designated Information Security Officer:

The Designated Information Security Officer (DISO) shall identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of ZMC data. This identification and risk assessment shall include adopting means for detecting security system failures and monitoring the effectiveness of the Computer System Security Requirements.

The DISO shall oversee the implementation of the Computer System Security Requirements and recommend changes to address risks, failures, or changes to business practices. The DISO shall work with other ZMC administrators to investigate any violation of this policy and any incident in which the security or integrity of College data may have been compromised, including taking the steps set forth below in response to a security breach. The DISO shall work with other ZMC administrators to develop and review training materials to be used for employee training under this policy.

Program Director:

The Program Director and Administrative Staff are responsible for promoting the institutional awareness of this policy and for ensuring overall compliance by their staff.

In particular, the Program Director and Administrative Staff are responsible for:

- Ensuring that all staff have the training and support necessary to protect data in accordance with this policy, all Data Security Directives, and any Specific Security Procedures applicable to such data.
- Designating and managing the efforts of Data Stewards for all Information Resources maintained in their area of responsibility.
- Approving access authorization of all Users of Information Resources maintained in their area of responsibility having a data classification of Confidential
- Promulgating Specific Security Procedures
- Ensuring that Confidential or Internal Use Only data sponsored within their area of responsibility are not provided or accessible to, or created or maintained by ZMC vendors or other third-parties without assistance from the DISO
    - Verifying that the third party has the capability of adequately protecting such data;
    - Review and approval of the relevant contract and the underlying terms and specifications by the DISO.

  - Verifying that the third party has executed ZMC’s standard form of Privacy and Security

Data Stewards:

Data Stewards are members of the ZMC community that have primary responsibility for maintaining any particular Information Resource. The Program Director or President may designate sponsors in connection with their administrative responsibilities and may include collection, development or storage of information (as in the case of individual faculty members with respect to their own research data or student grades).

- Data Stewards have primary responsibility for overseeing the collection, storage, use and security of a particular Information Resource.
- In cases where a Sponsor is not identified for any Information Resource, the cognizant Program Director shall be deemed the Data Steward.
- A Data Steward is responsible for the following specific tasks associated with the security of the information.
  - Ensuring that the Information Resource is assigned a security classification and that such data is marked where appropriate.
  - Identifying authorized Users of the Information Resource, whether by individual identification or by job title, and obtaining approval for such access from the Program Director.
  - Proposing to the Program Director specific Security Procedures for the handling of data under their sponsorship, consistent with this policy and other applicable ZMC policies and procedures.

Users:

Users include all members of the ZMC community to the extent they have authorized access to the school Information Resources. They may include students, faculty, staff, contractors, consultants and temporary employees and volunteers. Users are responsible for complying with all security-related procedures pertaining to any Information REsource to which they have authorized access.

Specifically, a User is responsible for:

- Becoming familiar with and complying with all relevant ZMC policies, including without limitation, this policy and all Data Security Directives contemplated hereby , the policy on Professional Standards, and Business Conduct and other policies related to data protection, technology use and privacy rights.

- Providing appropriate physical security for information technology equipment, storage media and physical data.

Access Control

Access to electronically stored PII is restricted in both ZMC's data management systems and in all data management systems in place from the U.S. Department of Education. Data contained in ZMC files is stored in a locked and secured storage area and also under the information security policies of the Google Drive platform and by ZMC's third party FSA servicer, GEMCOR. The information stored by GEMCOR is secured in the company's TEAM software. (see GEMCOR's policy on Data Protection and Security.. Each ZMC employee is required to maintain a unique User Account for accessing student information. ZMC's President and Program Director are the parties responsible for data security and protection at ZMC and are the only individuals authorized to create user accounts for ZMC's employees. User passwords are changed every 90 days.

Access to student information stored within USDE managed web sites requires unique FSA User Accounts and two-factor authentication. ZMC employees FSA User Accounts are created by ZMC's President, and SAIG secondary point administrator. The sharing of user IDs and/or passwords of any account used to access protected information is strictly prohibited and will result in disciplinary action, which may include termination of employment.

ZMC employees are required to only remain logged in to systems containing protected information during the time they are at their computer and actively accessing such systems. The display of any PII on computer monitors is to be minimized whenever possible. Should the need arise for an employee to leave their immediate work area, even temporarily, he/she must logout of all active sessions. Protected data may not be removed from the promises, physically or electronically, for any reason other than as required by job responsibilities. The DISO shall have the responsibility of ensuring adequate back up control which will routinely provide for the removal of protected data for temporary, off-sight storage. Fireproof safes shall be used for the storage of backup companies of all computer files, which contain PII.

In the event that any ZMC employee is no longer employed by the company or has been determined to no longer require access to protected information for the performance of his/her job responsibilities, ZMC management will immediately terminate the employee's user account(s).

Access to protected information stored in hard copy format within the offices of ZMC is restricted from unauthorized individuals and is not permitted without escort by an authorized ZMC employee whereby activity will be continually monitored. ZMC is protected by security monitoring cameras. Periodically, hard copy data maintained by ZMC is permanently disposed of through the employment of a licensed document destruction service.

Awareness & Training

ZMC staff and management are required to maintain awareness of data security and act as fiduciaries in the protection of such information. Failure to maintain such awareness can jeopardize students' information leading to identity theft. Managers, systems administrators, and users of organizational information systems are trained regarding the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems. Any change in such systems or in ZMC's file storage procedures will result in prompt training of staff to ensure the continued application of data security policies. New employees will complete a training session about information security policies and procedures at the time thier user accounts have been authorized.

Risk Assessment

A periodic review of ZMC's data protection and security policies is performed to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of client or student information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information. The review shall serve to assess the sufficiency of safeguards in place to control these risks. Potential risks will be evaluated in the areas of;

- Employee training and management;
- Information systems, including network and software design, as well as information processing, storage, transmission, hard copy file storage, and disposal
- Detecting, preventing, and responding to attacks, intrusions, or other system failures
- Testing existing data security mechanisms to ensure functionality

In the event that a risk assessment exercise indicates a potential risk to the protection of student protected information, an immediate analysis of the risk will be conducted and policies and procedures will be modified to restrict any exposure of protected information.

Data Transfers

Data transfers occur frequently between ZMC and its third party processor for FSA, GEMCOR. Due to such frequency, both ZMC and GEMCOR have automated processes and secure file sharing services to ensure the protection and safety of students personally identifiable information (PII). The procedures in place ensure data security regarding data transfers between GEMCOR and ZMC.

Data transfers between GEMCOR and ZMC are sent via secure document transfer protocols in place under Citrix's Sharefile service. PII is never included in the text of an email. Any email attachments containing PII are automatically password protected, encrypted with 256-bit Advance Encryption Standard (AES) algorithms, and are compressed using WinZip. Passwords necessary to open and access the contents of the attachment are never disclosed in the same email containing the attachment.

Data transfers containing PII originating at ZMC for submission to GEMCOR are performed using Citrix ShareFile file sharing service. See the GEMCOR Data and Security Policy. ZMC has a unique and dedicated folder in the ShareFile network into which files are deposited by authorized ZMC users.

Usage and Security Measures Regarding FSA Related Data Systems

Access to any USDE controlled data system such as COD, SAIG, G5, FAA Access, NSLDS, etc., requires the use of an FSA User ID, password and two factor authentication code. Each ZMC employee with access to any of the above systems, shall be assigned his/her unique FSA User ID for access to these systems. The following policies are in place regarding the use of FSA User IDs to access federal data systems.

- SAIG computing resources are used only for official ZMC business.
- Consumer information access with a ZMC FSA User ID is limited to applicants, students, student's parent(s), or prospective students of ZMC only for the purposes necessary in relation to the determination of aid eligibility of the individual.
- Only an authorized Destination Point Administrator is permitted to use the National Student Loan Data System (NSLDS).
- Only USDE provided software shall be used to monitor SAIG mailbox activity. This software will keep track of who is using the Destination Point (TG Number/Mailbox), what information is being accessed, the date and time of access, and the batch number (if applicable).
- FSA Users understand and consent to the monitoring, recording and auditing, of their connectivity and acknowledge that information gained in this manner may be disclosed by the Department to an appropriate third-party (e.g., law enforcement personnel).
- FSA Users agree to protect all Federal Student Aid applicant information from access by or disclosure to unauthorized personnel. In the event of an unauthorized disclosure or

breach of applicant information or other sensitive information (such as personally identifiable information), the DPA will immediately notify Federal Student Aid at CPSsaig@ed.gov.

- FSA Users agree that password sharing, the sharing of system access, and the use of any tools that allow accesses to the SAIG are strictly prohibited.
- Access is provided only to systems, networks, data, control information, and software for which ZMC's FSA User is authorized.
- Procedures for sanitizing stored information are followed to ensure data security (e.g., overwriting electronic media that contain sensitive information before reuse).
- FSA Users are aware of and must comply with all requirements to protect and secure data from Departmental sources using SAIG.
- At least on an annual basis, ZMC will validate all DPA and user access rights for the organization.
- At least on an annual basis, ZM will monitor the organization's NSLDS user access by creating reports using the NSLDS Web site.
- Employees and management shall inform ZMC's President of any changes in a user's need for access to Federal Student Aid systems because of changes to job responsibilities or termination of employment. ZMC will immediately deactivate or delta user access rights for employees who no longer require access.
- FSA Users must report immediately to ZMC's President or Program Director any security incidents, potential threats, or vulnerabilities that involve Electronic Services.
- FSA Users must report to ZMC's President or Program Director any compromise, suspected compromises, or incidents of sharing of a password or any other authenticator.
- FSA Users must access only those systems, networks, data, control information, and software for which he or she is authorized.
- FSA Users must ensure that all Electronic Services information is marked according to its sensitivity and is properly controlled and stored.
- FSA Users must inform ZMC's President or Program Director if the user no longer needs access to a Federal Student Aid system (i.e., the individual is leaving his or her position or his or her job responsibilities have changed).
- FSA Users must not add code that might be harmful to the SAIG or Electronic Services

Specific FSA User Usage and Security Measures

The data contained in Federal Student Aid (FSA) systems is confidential and is protected by the Privacy Act of 1974 (as amended), and other applicable statutes and regulations. Protected information includes, but is not confined to, name, address, telephone number, Social Security number, date of birth, maiden name, and similar types of information that can be used to identify a specific person.

Access to FSA systems is granted to individuals whose specific job responsibilities include at least one of the following activities:

- Determining a specific student applicant's eligibility for Title IV student aid;
- Billing and collecting on a Title IV loan;
- Enforcing the terms of a Title IV loan;
- Billing and collecting on a Title IV grant overpayment;
- Submitting student enrollment information;
- Ensuring the accuracy of a financial aid or borrower record;
- Assisting with default aversion activities;
- Obtaining default rate information; and
- Obtaining Gainful Employment Information

Data contained within FSA systems may not be used for any other purpose, including the marketing of student loans or other products.

Protection of Data Contained within FSA Systems:

To comply with the rules and regulations regarding the Title IV aid programs, ZMC may at times need to keep records of information that it has obtained from an FSA system.

- Any information retrieved from FSA systems may be shared only with individuals expressly authorized to receive this information.
- Data must not be "screen scraped" or accessed by automated tools and used in any other program.
- All printed materials are to be marked as Personally Identifiable Information (PII). • All sensitive information existing in hard copy must be stored in a locked container in a limited or exclusive area, an access controlled electronic environment, or be under the physical control of an authorized individual.
- All inquiries on student/borrower data must be business related.
- Electronic files must be properly encrypted. The current encryption protocol is Advanced Encryption Standard (AES) 256-bit, in accordance with Federal Information Processing Standards (FIPS). Additional information can be located at: http://csrc.nist.gov/publications/fips/index.html
- Never save unencrypted information on an unsecured drive, including a computer's hard drive.
- Never access data unless a relationship exists with the student/borrower.

- Never leave computers logged on and unattended. Log off at the end of each session or use access control software (i.e., screen saver with password) during unattended use.
- Never email Privacy Act protected information except in an encrypted and password-protected attachment.
- Never provide a password in the same email as an encrypted document.
- Never view sensitive material while in a public place. The penalty for knowingly disclosing information to unauthorized individuals or willfully violating security standards is a misdemeanor with a fine up to $5,000. Be Aware: You will be required to agree to conform to the Rules of Behavior for use of FSA systems and agree to abide by the Privacy Act of 1974 (as amended). Penalties for violating FSA security procedures are severe for both users and the organizations they represent.
- The sharing of User IDs and passwords is a violation of the Rules of Behavior and will result in the individual, and potentially the organization (and/or servicer), permanently losing access to FSA Systems.
- The User ID is assigned to an individual, not the organization.
- Only the individual to whom the User ID is assigned can use that User ID to access FSA systems online.
- Each individual is responsible for protecting his or her access, password, and the data in FSA systems.
- At no time should an individual be asked to provide their FSA system User ID and password to anyone. • This includes the employee’s supervisor or management.
- Individuals who are asked to provide their User ID and password to anyone must contact the Customer Service Center for the system in question immediately.
- An eligible organization that allows unauthorized access to an FSA system will be considered to have violated its responsibilities and places itself at risk of losing access to Departmental systems and data, and to possible loss of eligibility to participate in the Title IV student aid programs.
- ZMC trains employees on the importance of maintaining the privacy of student aid related data, and reviews its policies, procedures, and agreements to ensure that it is in full compliance.

Personally Identifiable Information (PII)

PII is information that can be used to distinguish or trace someone's identity. It is any information about an individual maintained by an agency. PII includes, but is not limited to, education, financial transactions, medical history, criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, biometric records, and any other personal information that is linked or linkable to an individual.

It can include information such as:

- Social Security Numbers;
- Age;
- Home and office phone numbers;
- Birthdays;
- Marital status and spouse names;
- Educational history;
- Medical history;
- Demographics;
- Biometric information; and
- Financial information.

These are often found on:

- Office personnel lists,
- Medical records,
- Rolodex cards, and
- Electronic-based address books or contact records.

Even if the individual pieces of information seem harmless, one or two pieces of information can be combined with other information to compromise someone's identity. For example, the Social Security Number, if associated or combined with other PII, can create a high risk to the identity protection of an individual. In many FSA systems, PII is a subset of sensitive information. If you handle PII, you are the first line of defense in preventing identity theft. It is each ZMC employee and community members responsibility to protect any PII entrusted to them. ZMC works diligently to protect PII and mitigate the damage if PII is lost or stolen.

Sensitive Information:

Sensitive Information can include, but is not limited to:

- Personnel,
- Financial,
- Payroll,
- Medical,
- Operational, and
- Privacy Act information.

During working hours, reasonable steps should be taken to minimize the risk of access to sensitive information by unauthorized personnel. All sensitive information is stored in locked containers, desks, or cabinets or on password protected and locked systems.

Creating a Secure Password

Below are some general guidelines all ZMC staff and community members should follow to protect the Government's information systems from being compromised.

Using these guidelines at home keeps your home computer secure as well.

Password Do's:

- Do use a combination of: o Lower and upper case letters, o Numbers, and, o Special characters, such as the number sign or percent sign.
- Do change your password every 90 days.
- Do create a complex, strong password, and protect its secrecy. This is critical for protecting Federal information and information systems, as well as for protecting your own personal information.

Password Don'ts:

- Do not use personal information, such as: o Birthdays, or o Names of: - Family members, - Friends, - Pets, - Favorite sports teams, or - Favorite bands.
- Do not use common phrases or words found in the dictionary, including foreign languages. Hackers even have a Klingon dictionary!
- Do not write down your password. Commit it to memory.
- Do not share your password with anyone, ever.

Example of Strong Password

MH1&MomPlus3131 is the best option as it contains:

- Upper case letters,
- Lower case letters,
- Numbers, and
- Special characters.

Unlocked Computer

All ZMC Employees and Staff members are required to take the following precautions when leaving their workstation:

- Be sure to manually log off or shut down your computer when not actively monitoring your workstation.
- When you leave for the day, be sure to log off your computer.
- Turn off the computer at the end of the school's day.

Spillage

Spillage includes the improper handling of sensitive information on a non-sensitive system, including the improper:

- Storage
- Transmission, or
- Processing of information

When storing sensitive information, including PII, prevent spillage by following these security tips:

- Encrypt data before storing.
- Store data only on a network that has been certified and accredited to store this type of information.
- Remember, some systems are strictly non-sensitive. Never transmit, store, or process sensitive data on a non-sensitive system.

Social Engineering

Social engineering is a collection of techniques intended to trick people into divulging private information. The social engineer attempts to use the information to gain unauthorized access to computer systems, or to commit fraud.

Social engineers use a variety of communication devices to contact their victims, including:

- Telephone surveys,
- E-mail messages,
- Websites,
- Text messaging,
- Automated phone calls, and

- In-person interviews.

Phishing

Phishing is one type of social engineering that uses e-mail or websites to trick you into disclosing personal, sensitive information, such as:

- Credit card numbers,
- Bank account information,
- Your Social Security Number, or
- Passwords.

The intention is to steal your identity (identity theft), run up bills or commit crimes in your name, or access your organization's computer systems. Phishing is a serious, high-tech scam.

How does it work?

Phishers try to deceive you by sending e-mails or pop-up messages that appear to be from

- Your Government agency,
- Your Internet service provider (ISP),
- Your bank, or
- Some other legitimate business or organization.

The message might claim that you need to update or validate your account information. It might threaten some dire consequence if you do not respond. The message directs you to a web site that looks just like a legitimate organization's site, but it is not affiliated with the real organization in any way. The bogus site tricks you into divulging your personal information. It may also install malicious code on your system.

Removable Media

Removable media includes:

- CDs,
- DVDs,
- Thumb drives,
- Flash drives, and
- External hard drives.

Removable media that contains sensitive information must be properly:

- Labeled,
- Stored,
- Encrypted, and, when discarded,
- Purged.

If the media contains PII or other sensitive data, including Government information not cleared for public release, the information must be encrypted. Contact your security POC for additional information on proper labeling of removable media.

Be careful how you discard of CDs or other removable media. A CD that is labeled as sensitive must be purged before it is discarded. Merely deleting sensitive data does not prevent it from being recovered.

The most common purging method is using an approved software tool that repeatedly overwrites the entire media to destroy any recoverable remnants of the original information.

Anything that cannot be overwritten must be physically destroyed. For example, many shredders are designed to handle CDs and DVDs. Be aware that data can be recovered from media fragments as small as 1/100 of an inch. ZMC's DISO can help identify an appropriate data purging method based on the sensitivity of your information.

Mobile Computing Devices

ZMC staff and community should be extra vigilant when storing data on mobile computing devices, such as, PDAs, cell phones, laptops, and personal electronic devices, or PEDs. Because of their small size and portability, these devices are especially vulnerable to security risks.

All PDAs and other mobile computing devices connecting to Government systems must be in compliance with Federal policy. Please note that the Government considers laptop computers as mobile computing devices.

All laptops that store PII must be secured using a whole-disk encryption solution to protect the sensitive information stored on them.

All sensitive data must be encrypted in accordance with the data's sensitivity level. This includes all PII, such as:

- Social Security Numbers,
- Dates and places of birth,
- Mothers' maiden names, and
- Biometric records.

If a device is lost or stolen, immediately report the loss to your security POC. If the PDA contains PII, you must also follow any other procedures your organization has implemented regarding the compromise of PII.

Please note that some agencies may severely restrict or prohibit the use of mobile computing devices.

Fax Machines

Before transmitting sensitive information over a fax machine:

- Ensure that the recipient is at the receiving end, ready to pick up the fax immediately.
- Use the correct cover sheet for the sensitivity of the information you are faxing.
- After sending the fax, contact the recipient to confirm receipt.

Never transmit sensitive information via an unsecured fax machine

E-Commerce and Cookies

A cookie is a text file that a web server puts on your hard drive. As you enter information at a website, the cookie saves the data, including which items you've placed into your "shopping cart," your user preferences, and your username.

Though sometimes useful, enabling cookies can pose a security threat, the most serious being when a cookie "saves" unencrypted personal information, such as your credit card numbers or Social Security Number.

Cookies can also track your activities on the web; this also poses a security risk and may lead to a potential invasion of your privacy.

Both in the office and at home, shop online wisely and follow these security tips:

- Use cookies with caution.

- If your organization does not configure your cookies setting, set your browser preferences to prompt you each time a website wants to store a cookie.
- Only accept cookies from reputable, trusted websites.
- Confirm that any e-commerce site conducts its business over an encrypted link before providing any personal information:
- An encrypted link is indicated by "h-t-t-p-s" in the URL name.
- Make sure that an icon is visible that indicates the encryption is functioning. Note that not all https sites are legitimate; you are still taking a risk by entering your information online.

Additional Information for PDPAs:

If you have been identified as a PDPA for your organization, in addition to the information listed above you are responsible for:

- Enrolling the organization's users.
- Maintaining an accurate and current listing of your organization's active users.
- Deactivating users who are no longer employed or whose job no longer warrants access to FSA systems.
- Monitoring users' access for any unauthorized activity.
- Recertifying online access for your organization's users on an annual basis.
- Signing access applications that your servicer makes through www.fsawebenroll.ed.gov

You should never approve a user for access unless that person is an employee of the organization, school, or servicer to which the school has contracted to perform necessary functions. In addition, you must promptly deactivate any user who loses eligibility.

Questions: Please feel free to contact ZMC’s designated Data Protection Officer at rebecca@zmc.edu for more information.

Copyright Infringement & Acceptable Use Policy

Zion Massage College retains the copyright to all curricular and support material, which is provided to students, in our program. ZMC retains the copyright to all curricular and support material created for its program, and also holds liable those who would infringe upon the exclusive rights of all supplementary copyrighted materials. Unauthorized distribution of copyrighted material, including peer-to-peer file sharing, is prohibited and may subject a student to civil and criminal penalties. Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement. Penalties for copyright infringement include civil and criminal penalties, including payment of either actual or statutory damages, organizational attorney fees and court costs. For details, see Title 17, United States Code, Sections 504, 505. For more information, please see the Web site of the U.S. Copyright Office at www.copyright.gov.

Acceptable Use Policy

To support our students in their learning process, ZMC provides computing, networking and information resources to it’s students and staff members. Please note that access to ZMC facilities is a privilege, which is conditioned upon your compliance with the school’s current Acceptable Use Policies. ZMC expects students and staff members to act responsibly when using the school’s computers and other resources.

Students and staff members have promised to know and to follow all ZMC policies and are bound by the ZMC Conduct code. Please honor your commitment by carefully reading and following the school policies.

ZMC users are liable for any and all activities while logged on to a school computer or using other school resource materials. All school policies and regulations along with relevant federal and state laws apply.

Examples of misuse include, but are not limited to, the activities in the following list.

- **Copyright infringement.** Please note that reproduction or distribution of copyrighted works, including, but not limited to, images, text, or software, without permission of the owner is an infringement of U.S. Copyright Law and is subject to civil damages and/or criminal penalties including fines and imprisonment.
- **Violation of campus regulations and/or applicable federal or state laws**, including but not limited to visiting sites or viewing any material that might reasonably be deemed obscene or pornographic, the transmission of threats, harassment, defamation; theft of or unauthorized access or use of University resources; conduct unreasonably obstructing or disrupting teaching, learning or research.
- **Using resources or accounts other than your own, engaging in activities which compromise computer security or disrupt services, at any site.** Including but not limited to: Using resources or accounts without authorization. Capturing passwords. Collecting or using tools designed to check for computer system or network security vulnerabilities.
- **Altering** ZMC system software or hardware configurations or circumventing resource control mechanisms.
- **Knowingly running or installing** on any computer system or network, or giving to another user, **a program intended to damage or to place excessive load** on a computer system or network. This includes but is not limited to programs known as computer viruses, Trojan horses, and worms.
- **Using facilities for commercial purposes**, or personal financial gain (except where permitted by academic policy). This includes setting up a commercial Web site on your personal computer which is made accessible to the world via a connection to the UCSD network.
- **Sending electronic junk mail or chain letters**.
- **Posting material** to electronic bulletin boards, news groups, or mail lists which is illegal, or otherwise at variance with applicable codes or rules for network access and use (e.g. Usenet rules published in news.announce.newusers).

- **Preventing others from doing their work** and wasting resources by tying up equipment for periods longer than 2 hours, downloading files onto ZMC computers or running compute intensive software or jobs.

Enforcement

Violations of ZMC policies may result in the loss of computing and other resource material privileges. Additionally violations may subject the student to disciplinary action under ZMC regulations and/or criminal prosecution if applicable.