Overall Structure of Program

I. Background

a. Purpose

The Federal Trade Commission (FTC) requires financial institutions to establish policies and procedures for safeguarding customer financial information by complying with the Gramm-Leach-Bliley Act (GLBA). The GLBA also includes specific requirements regarding the privacy of customer financial information. The FTC has ruled that being in compliance with the Family Educational Rights and Privacy Act (FERPA) satisfies the privacy requirement of the GLBA, but does not satisfy the safeguarding provisions. This procedure focuses on the safeguarding of customer information.

b. Authority

EWC Board of Trustees adopted Board Policy 6.8 and EWC Administrative Rule 6.8.1 to comply with the requirements of the Gramm-Leach-Bliley Act and thereby grant the Designated Security Program Officer the authority to implement this Information Security Program.

c. Objectives

- Ensure the security and confidentiality of customer records and information.
- Protect against unauthorized access to, or use of, such records or information that could result in substantial harm or inconvenience to any customer.
- Protect against any anticipated threats to the security or integrity of such records.
- Minimize identity theft.

d. Definitions

- **Customer information** is defined as any record containing nonpublic, personal financial information, whether in paper, electronic, or other form, that EWC obtains from a student or other third party, in the process of offering a financial product or service. Examples of customer information include names, addresses, phone numbers, bank and credit card account numbers, income and credit histories, academic and employment information, and social security numbers. In general, the **financial products or services** offered by a college or university include making student loans, processing tuition payments, and other miscellaneous financial services.
- **Covered data** is defined as all information required to be protected under GLBA. This includes **customer information**, as well as financial information that the College, as a matter of policy, has included within the scope of this Information Security Program, whether or not such information is covered by GLBA. This may include financial and personal information obtained by the College outside of a financial service transaction.
- **Service providers** are defined as all third parties who, in the ordinary course of EWC business, are provided access to covered data. Examples of service providers include businesses retained to transport and dispose of covered data, collection agencies, and systems support providers.

II. Information Security Program Components

a. Designated Security Program Officer

The Vice President of Financial Affairs has been designated as the Program Officer and is responsible for coordinating and overseeing the Program. The Program Officer may designate other employees at EWC to oversee and coordinate particular elements of the Program. Any questions regarding the implementation of the Program or the interpretation of this document should be directed to the Program Officer.

b. Risk Identification and Assessment

EWC intends, as part of the Program, to identify and assess external and internal risks to the security, confidentiality, and integrity of nonpublic financial information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information. In implementing the Program, the Program Officer will establish procedures for identifying and assessing such risks in each relevant area of EWC's operations, including:

i. Employee Training and Management

The Program officer will coordinate with representatives of EWC's Human Resources Department, Business Office, Computer Services Department, and Financial Aid Office to evaluate the effectiveness of EWC's procedures and practices relating to access to and use of student records, including nonpublic financial information. This evaluation will include assessing the effectiveness of EWC's current policies and procedures in this area.

ii. *Information Systems and Information Processing*

The Program Officer will coordinate with representatives of EWC's information/computer technicians by and through the Vice President/Dean of Instruction to assess the risks to nonpublic financial information associated with EWC's information systems. This evaluation will include assessing EWC's current policies and procedures relating to the use of the network and network security. The Program Officer will also coordinate with the Vice President/Dean of Instruction to assess procedures for monitoring potential information security threats associated with software systems and for updating such systems by, among other things, implementing patches or other software fixes designed to deal with known security flaws.

iii. *Detecting, Preventing, and Responding to Attacks*

The Program Officer will coordinate with EWC's Vice President/Dean of Instruction to evaluate procedures for and methods of detecting, preventing, and responding to attacks or other system failures, and existing network access responses to network attacks and developing incident response teams and policies. In this regard, the Program Officer may elect to delegate to a representative of the Vice President/Dean of Instruction that responsibility for monitoring and participating in the dissemination of information related to the reporting of known security attacks and other threats to the integrity of networks utilized by EWC.

iv. *Document Retention, Security, and Disposal*

The Program Officer will assess file management practices wherever nonpublic financial information is found to ensure that adequate systems are in place to protect sensitive documents from unauthorized use and provide archive and/or disposal plans for documents and files that are no longer needed.

c. Security Provisions and Safeguards

With respect to the safeguarding provisions of the GLBA, the Eastern Wyoming College GLBA Information Security Program herein is designed to ensure the security, integrity, and confidentiality of non-public customer information, protecting it against anticipated threats, and guarding it against unauthorized access or use. Covered under the Program are technical and physical safeguards used in the collection, distribution, processing, protection, storage, use, transmission, handling, or disposal of non-public customer information. The Program covers actions by both employees of the College and outside service providers. The policies incorporated in this document apply to all College departments. In addition, in the case that individual departments may have additional security provisions, they will maintain written documentation of these and will make them available to the Security Program Officer.

The following is a list of threats to customer financial information that will be mitigated through the implementation of this plan:

1. Unauthorized access to data through software applications.
2. Unauthorized use of another user's account and password.
3. Unauthorized viewing of printed or computer displayed financial data.
4. Improper storage of printed financial data.
5. Unprotected documentation usable by intruders to access data.
6. Improper destruction of printed material.

The College safeguarding policies include the elements described in the following sections.

i. Technical Safeguards

1. Electronic access to customer financial information is protected by usernames and passwords and such rights are restricted based on a user's status.
2. EWC Computer Services provides network security and administrative software password access security according to industry standards.
3. Passwords are to be kept confidential. They will not be taped to computer monitors, put under keyboards, or on a sticky note inside a desk drawer.
4. Passwords are not to be shared by other users. Students requiring access to customer financial information are given their own account and password with appropriate privileges assigned.
5. Network passwords (for logging into Windows) expire every 180 days. When changing passwords, employees are to choose passwords that are of a complex nature and that are sufficiently different from previous passwords.
6. Passwords to login to Datatel Colleague (DEC) are to be of a complex nature (ex. DES!t1). All password changes for Datatel must be coordinated through the Assistant Director of Computer Services and must always meet the criteria for complex passwords.
7. EWC Computer Services has created a directory structure for employees to save electronic files. The structure of such directories allows employees to determine whether files can be viewed by anyone on the network (Public folder), by only Work Study students and department employees in that area (Work Study folder), by department employees only (Staff folder), or on a drive to which only the individual employee has access rights. As an example, access to customer financial information on the network for the Business Office area Staff folder is safeguarded with access rights granted to employees with Business Office authorization.
8. Electronic files containing non-public information are not saved in a Public Folder on the network.
9. Whenever possible, electronic files of non-public information are viewed on the shared network drives that are secured based on network access settings. If an employee needs to share the file with someone they do not share a network drive with, employees are encouraged to password-protect electronic files of non-

public information when emailing or to transport data via jump drive, CD-ROM or disk.

10. EWC Business Office uses secure, password-protected systems, and encrypted transmissions outside the College, such as Zix Mail, for covered data. Other EWC offices that send electronic transmissions outside the College also use password protected/encrypted transmission systems.
11. All electronic non-public information should be password protected if stored anywhere other than on the network (e.g., external drives, laptops, etc).
12. In-bound Internet traffic is monitored for intrusion attempts.
13. EWC Computer Services assists departments with repairing computing systems that have been hacked and issues notifications and takes appropriate actions to protect the College networked resources if it occurs.
14. Vulnerability scans of networks are performed regularly.
15. Virus and spyware protection updates are provided.
16. Virtual Private Network (VPN) and Verisign certificates are used to protect the security of the College's data network and for ensuring the validity of vendor supplied program updates.
17. All security and privacy incidents shall be reported to Computer Services and Program Office and will be researched and resolved.
18. Patches to correct software vulnerabilities are regularly obtained and installed.
19. EWC Computer Services permanently removes or otherwise destroys covered data from computers, diskettes, magnetic tapes, hard drives, or other electronic media prior to disposal.
20. Employees shall turn off computers at the end of every day 1) to allow for all network files to be backed up, 2) to allow for updates to be installed when computers are subsequently turned back on, and 3) to prevent unauthorized access to the employee user accounts.
21. Back-up tapes of the EWC network and the administrative data are stored in the College's off-site safe deposit box. Back-up tapes are made daily and deposited weekly.
22. EWC will maintain an Information Security and Privacy web page http://ewc.wy.edu/administration/infosecurity to be a reference for the College and those outside of the College interested in this Program.
23. Covered data is collected and displayed through EWC's website by user-initiated transactions. Data is encrypted and Verisign certificates are used to protect the data. 1) Some of that data is transient in nature and is deleted when the transaction is complete or after approximately 20 minutes if the transaction is abandoned. 2) Some of that data is collected for internal use and remains resident on the server until the end user deletes it. It is recommended that these data be reviewed at least annually for continuing relevance and deleted as necessary. Departments that utilize such stored data maintain a procedure detailing the deletion schedule. Back-ups of these data are maintained with the same physical security as the web server itself.

ii. Physical Safeguards

1. The College uses direct personal control or direct supervision to control access to and handling of all non-public customer information when an office is open. Whether the information is stored in paper form or any electronically accessible format, departmental non-public information is maintained, stored, transmitted and otherwise handled under the direct personal control of an authorized employee of the College.
2. Departmental non-public information is collected, processed, transmitted, distributed and ultimately disposed of with constant attention to its privacy and security.
3. Key access is limited to authorized College employees only, in the context of College key control governing the distribution of keys.
4. Confidential material is kept secure. Most offices have locked windows and locked doors with restricted access. For those that do not, materials are kept in locked filing cabinets or other locked storage areas. Offices and/or computers are locked when someone is not present in the office.
5. When offices are open, confidential information is kept out of sight from visitors, and computer terminals are placed in such a way that visitors cannot see what is on the screen.
6. Computer terminals used to display customer financial information are not to be left unattended with that information still displayed.
7. All users must set their screensaver to initiate after thirty minutes to lock the computer screen requiring a password to reactivate. All users shall use Task Manager to lock the computer if they will be leaving their work area.
8. Conversations concerning non-public information are held in private. Employees are to be conscientious if a closed door is not possible that they are taking steps not to compromise students' privacy. Use of ambient background noise is encouraged to aid in the prevention of others overhearing private conversations.
9. Papers with non-public information are mailed via official campus mail, US mail, or private mail carrier. If a customer makes arrangements to pick up such papers, the customer must present a photo ID.
10. Outdated records are disposed of according to the Wyoming State Archives schedule. When non-public information is disposed, it is destroyed; paper containing such information is routinely shredded or otherwise destroyed.
11. Onsite storage of physical records in closets or vaults are locked and secured with limited access. The College offsite storage is limited to a local bank safe deposit box and the Wyoming State Archives. Such storage is safeguarded the same as onsite storage.
12. Physical and electronic records are protected from physical hazards such as fire or water damage by storing records in fireproof filing cabinets or vaults.

iii. Training

1. Training for new staff will include an explanation of the purpose of the GBLA and a copy of this plan. Each staff member will sign that he/she has received a copy

of this plan and that he/she understands his/her responsibilities under this plan. This statement will be filed in the Personnel Office. In addition, all other applicable forms, as mentioned above, must be signed before access is granted to customer financial data.

2. Existing staff will receive the same training as new staff and be reminded each year at the fall in-service of their responsibilities under the GLBA.
3. Student employees will undergo training from their supervisor and will be reminded of their obligations when they stop working for the College. Each supervisor will get a signed statement by the student that he/she received a copy of the plan and that he/she understands his/her responsibilities under the plan. The signed statement will be kept by the Financial Aid Office.
4. All College employees, including part-time and temporary employees, and volunteers are given specific training by their supervisors about issues of security of sensitive and confidential material used in their respective offices.
5. Employees are held accountable to know the provisions and their responsibilities set forth in this Program. Non-compliance with the safeguards of this Program will be noted in an employee's annual performance evaluation and other disciplinary action may be taken.
6. Employees are held accountable to know that although they have access to non-public information in order to perform their duties for the College, they are not permitted to access it for unapproved purposes or disclose it to unauthorized persons.
7. EWC will maintain an Information Security and Privacy web page http://ewc.wy.edu/administration/infosecurity to be an educational tool and resource for employees of the College as they comply with this Program.
8. EWC will develop and publish a pamphlet for the College community on tips for keeping non-public information secure.

Overseeing Outside Service Providers

1. Each area will assure that third party service providers are required to maintain appropriate safeguards for nonpublic information to which they have access. Any Request For Proposal (RFP) and resulting contracts with service providers, who within their contracts would have access to Eastern Wyoming College non-public customer information, shall include the following, as appropriate:
    a. A description of the legitimate educational interest or institutional business function served by access to covered data;
    b. Explicit acknowledgment that the contract allows the contract partner access to confidential information;
    c. Specific definition of the confidential information being provided;
    d. Stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract;
    e. Guarantee from the contract partner that it will ensure compliance with the protective conditions outlined in the contract;
    f. Guarantee from the contract partner that it will protect the confidential information it accesses according to commercially acceptable standards

and no less rigorously than it protects its own customers' confidential information;

g. Stipulation that the contractor will comply with any and all state and federal privacy laws;
h. Provision allowing for the return or destruction of all confidential information received by the contract partner upon completion of the contract;
i. Stipulation allowing the entry of injunctive relief without posting bond in order to prevent or remedy breach of the confidentiality obligations of the contract;
j. Stipulation that any violation of the contract's protective conditions amounts to a material breach of contract and entitles Eastern Wyoming College to immediately terminate the contract without penalty and should describe the lawful penalties for misuse or inappropriate disclosure of that information;
k. Provision allowing auditing of the contract partners' compliance with the contract safeguard requirements; and,
l. Provision ensuring that the contract's protective requirements shall survive any termination agreement.

2. EWC will develop and send to each covered service provider a form letter that requests assurances of GLBA compliance.

Adjustments/Reassessment of Plan/Periodic Review and Adjustment of Program

The Program Officer is responsible for evaluating and adjusting the Program based on the risk identification and assessment activities undertaken pursuant to the Program, as well as any material changes to the Institution's operations or other circumstances that may have a material impact on the Program.