Policy Series 3000
Policy 3005
Procedure 3005.1
Data Security Information Program

I. Purpose and Background

In order to protect confidential information and data, and to comply with federal laws, this document summarizes the Northern Wyoming Community College District (NWCCD or District) comprehensive written information security and identity theft prevention procedure. The Gramm-Leach-Bliley Act of 2000 (GLBA) mandates that financial institutions must take steps to safeguard the security and confidentiality of customer information. The Federal Trade Commission (FTC) ruled that GLBA applies to institutions of higher education. Compliance with GLBA involves compliance with 1) the privacy provisions of the Act, and 2) provisions regarding the safeguarding of customer information. The Fair and Accurate Credit Transactions Act (FACT Act) requires financial institutions to establish a program to help detect, prevent, and mitigate identity theft of "covered accounts." The FTC has said that colleges are deemed in compliance with the privacy provisions of GLBA if they are in compliance with the Family Educational Rights and Privacy Act (FERPA). With respect to the second area, GLBA and the FACT Act specify new requirements for colleges to safeguard non-public customer information and certain covered accounts, such as family financial information, social security and identification numbers, by having an institutional security program and security plans in specific offices of the college that handle such information.

II. Gramm-Leach-Bliley and FACT Act Requirements

GLBA mandates that the District designate information security program representatives to coordinate the information security program, conduct a risk assessment of likely security and privacy risks, institute a training program for all employees who have access to customer information, oversee service providers and related contracts, and evaluate and adjust this program periodically. The FACT Act has similar requirements, including mandating schools to have a program to identify, detect, and respond appropriately to relevant "red flags;" this is further detailed in *Procedure 3015.2: NWCCD Identify Theft Program*.

III. Designated Security Program Officers – Colleague Manager's Group

The members of the Colleague Manager's Group are the designated GLBA Security Program Officers for the District and are listed here.

- Assistant Vice President, ITS/Chief Information Officer, Co-chair
- Assistant Vice President, Enrollment Management/Registrar, Co-chair

- Assistant Vice President, Human Resources
- Executive Director, Admissions
- Director, Finance/Controller
- Director, Financial Aid
- Director, Advising Services
- Director, Administrative Services, Gillette College
- Director, Enrollment Services, Gillette College

The following positions provide support, leadership and are a resource to the Colleague Manager's Group to ensure appropriate data security protocols for their designated areas:

- Assistant Vice President, Facilities
- Director, Facilities, Gillette College
- Director, Dental Hygiene (HIPAA Compliance for the Dental Clinic)
- Clinic Manager, Dental Hygiene (HIPAA Compliance for the Dental Clinic)

The Colleague Manager's Group and the individuals who serve as the GLBA security program officers provide leadership to the administration and maintenance of the procedures and processes included in the data security information program, the identity theft prevention plan, and the information technology services security procedure as outlined in this procedure and *Procedure 3005.2: Identify Theft Prevention Program* and *Procedure 3005.3: Information Technology Services Security*.

The Colleague Manager's Group members provide leadership to campus-wide data security efforts and advisory support to ITS staff in these endeavors. This includes the management of the following processes:

1. Maintenance of the *Data Security Training Guide* which provides a general overview of the District systems, definitions, remote access considerations, and processes for reporting a data breach.
2. Administration of the annual employee training and prevention program.
3. Annual review of the Federal Financial Institutions Examination Council cybersecurity and preparedness assessment.
4. Development of an annual monitoring report to the NWCCD Board of Trustees that includes preventative activities, risk assessment, data breaches, and future initiatives.

IV. Customer Information

For purposes of FERPA and GLBA, the District considers students, employees, alumni, and any other third party engaged in a financial transaction with NWCCD as "customers." Customer information that must be safeguarded is "any record containing nonpublic personal information about a customer, whether in paper, electronic, or other form." It includes financial information,

student’s financial accounts, academic and employment information, and other private paper and electronic records.

V. Privacy Provisions

With respect to the privacy provisions of the GLBA, NWCCD complies with FERPA. Directory information (name, address, enrollment at the college and degree information) is considered public, unless a student has requested otherwise in writing. All non-directory information is restricted or confidential, what GLBA calls "non-public." Under FERPA, restricted information (for example, academic or financial records) is released outside the District only with the student's written consent. Designated school officials, including faculty, key employees and occasionally outside service providers, have access to restricted, “non-public” information on a need-to-know basis only. Confidential information (for example, a faculty member's or department chair’s private notes) is even more protected than restricted information and released only in certain unusual circumstances as outlined in FERPA.

In addition, the District complies with HIPAA (Health Insurance Portability and Accountability Act of 1996) with respect to the dental hygiene clinic. The academic department director provides leadership to ensure that patient information is secured in accordance with all privacy guidelines.

VI. Security Provisions

With respect to the safeguarding provisions of the GLBA Act, this procedure 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. This procedure applies to all District departments and covers all physical, technical, and administrative safeguards used in the collection, distribution, processing, protection, storage, use, transmission, handling, or disposal of non-public customer information.

VII. Physical Safeguards

The District 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 District.

Departmental non-public information is collected, processed, transmitted, distributed, and ultimately disposed of with constant attention to its privacy and security. Conversations concerning non-public information are held in private. Papers with non-public information are

mailed via official campus mail, US mail, or private mail carrier. Departments are encouraged to password-protect electronic files of non-public information when transmitting electronically. When best practices permit the disposal of non-public information, it is destroyed; paper containing such information is routinely shredded.

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. When offices are open, confidential information is kept out of sight from visitors, and computer screens are not visible to visitors. Offices and/or computers are locked when the office will be vacant for an extended length of time.

Key access is limited to authorized District employees only, in the context of District key control governing the distribution of keys. Campus Police further ensures the security of offices after hours.

Departmental cloud storage and information processing generally conforms to the same practices as onsite storage and is safeguarded under the provisions for outside service providers, as described below.

VIII. Technical Safeguards

Procedure 3005.3: Information Technology Services Security outlines the technical safeguards managed by the Information Technology Services Department (ITS). According to industry standards, the District relies on the ITS to provide network security and administrative software password access security. This protects non-public student information that is accessed electronically but stored outside of a department. Departmental desktop computers and other electronic devices storing non-public student information are protected by physical safeguards.

IX. Employee Management and Training

All District employees including part-time, temporary, student employees, and volunteers are trained when they are hired and are provided annual training thereafter in reference to security of sensitive and confidential material used in their respective offices. Employees are held accountable to know and understand that they are not permitted to access non-public information for unapproved purposes or to disclose it to unauthorized persons. Their access is only to perform their duties for the District. The training includes processes to detect and not respond to "pretext calling" or e-mail "phishing" which occurs when someone attempts to obtain confidential information via unauthorized calls or electronic means in order to commit identity theft. The Employee Handbook articulates that violation of security policies could result in disciplinary action up to and including dismissal from employment, legal action, or both.

X. Outside Service Providers

ITS shall guide the entire purchasing process of their-party software services to manage the contract details pertaining to data ownership, security, stewardship, and backup. All contracts must be reviewed by both the director of the functional area requesting the contract and the Chief Information Office prior to VP of Administration/CFO approval. Each area ensures that third party service providers are required to maintain appropriate safeguards for no-npublic information to which they have access. Contracts with service providers, who within their contracts have access to NWCCD non-public student information, shall include the following provisions:

- Explicit acknowledgment that the contract allows the contract partner access to confidential information;
- Specific definition of the confidential information being provided;
- Stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract;
- Guarantee from the contract partner that it will ensure compliance with the protective conditions outlined in the contract;
- 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;
- Provision allowing for the return or destruction of all confidential information received by the contract partner upon completion of the contract;
- Stipulation allowing the entry of injunctive relief without posting bond in order to prevent or remedy breach of the confidentiality obligations of the contract;
- Stipulation that any violation of the contract's protective conditions amounts to a material breach of contract and entitles NWCCD to immediately terminate the contract without penalty;
- Provision allowing auditing of the contract partners' compliance with the contract safeguard requirements;
- Provision ensuring that the contract's protective requirements shall survive any termination agreement.

XI. Review, Reporting, & Assessment Procedure

An annual assessment of data security occurs annually. The assessment includes the review of the procedures that are included as part of *Policy 3005: Data Security* by the Colleague Manager's Group. The GLBA Security Program Officers circulate these procedures to each department and request a review and assessment. The annual review also includes identification

and assessment of internal and external risks to the security, integrity, and confidentiality of non-public customer information and covered accounts, including review of outside contractors and their contracts to ensure that proper safeguards are in place. The results from each department will be included in a comprehensive review of the District. These reports are used to inform improvements to the systems and training priorities. A summary of these reports is provided to the NWCCD Board of Trustees in an annual monitoring report.