REGULATION on Identity Theft Prevention Number 2.17.2

The risk to the district, its employees and customers from data loss and identity theft is of significant concern to the College and can be reduced only through the combined efforts of every employee and contractor.

Under the Red Flags Rule, the College is required to establish an “Identity Theft Prevention Program” tailored to its size, complexity and the nature of its operation. The program must contain reasonable policies and procedures to:

1. Identify risks that signify potentially fraudulent activity within new or existing covered accounts;

2. Detect risks when they occur in covered accounts;

3. Respond appropriately to risks that are detected to prevent and mitigate Identity Theft; and

4. Update the program periodically, to reflect changes in risks to students and other College constituents from Identity Theft.

The College appointed Internal Information Security Awareness committee, will oversee, train, and update the Identity Theft Prevention Program.

In June 2015, the “Red, Yellow and Greed Document Classification” procedure was put in place and is summarized as follows:

- **Red**: Documents that contain sensitive/confidential information. Personally identifiable information (PII, as used in US privacy law and information security, is information that can be used on its own or with other information to identify, contact or locate a single person, or to identify an individual in context) always needs to be saved as red. These documents will be stored on a local file server and can be accessed only from campus.
- **Yellow**: Documents that are not sensitive or confidential but are internal and not public information. These documents will be stored on SharePoint team sites in Office 365 and are made accessible via sharing permission to authorized faculty and staff.
- **Green:** These are public documents that are viewable on the College website.