CCBC
The Community College of Baltimore County

Privileged Access and
Ethical Data Handling Agreement

April 2008

1.0 Introduction and Purpose

System administrators and managers of the Community College of Baltimore County (CCBC) Information Technology Services (ITS) department, have the additional responsibility of ensuring the integrity, confidentiality, and availability of the resources they are managing. Persons in these positions are given broader access to computer systems and resources because their job responsibilities require such access. These individuals are granted significant trust to use their privileges appropriately for their intended purpose, and only when necessary to maintain the system. Any private information seen in carrying out these duties must be treated in the strictest confidence, unless it relates to a violation or the security of the system.

2.0 Related Policy References

The details in this agreement are additions to the responsibilities acknowledged by all computer users, contained in the following policies:

a. CCBC Acceptable Use Policy
b. CCBC Wireless Policy
c. CCBC Data Security Policy
d. CCBC Privacy & Security Policy
e. CCBC Password Protection Policy

3.0 Privileged Access

Only those employees requiring special access to perform job responsibilities shall be eligible for elevated privileges and/or increased access to files and records. Eligible employees must sign this agreement prior to receipt of a username and password granting privileged access. Your signature below constitutes your acknowledgement that username and password information granting privileged access is strictly confidential and is not subject to disclosure under any circumstance, except with the express approval of the CIO.

4.0 Employees with Privileged Access to CCBC Computing Resources Agree:

a. Not to “browse” through the computer information of system users while using the powers of privileged access, unless such browsing is a specific part of their job description (e.g. computer auditor); is required during file system repair, management, or restoration; is necessary to investigate suspicious or system-impairing behavior; or is specifically requested by, or has the approval of, the person who authorized the privileged access. Authorizers of this access are Deans, VP’s, CIO, and/or Directors.
b. Not to disclose, to any unauthorized person, computer information observed while operating with privileged access.
c. Not to copy any computer information for any purpose other than those authorized under their defined job responsibilities.
d. Not to intentionally or recklessly damage or destroy any CCBC computing resource.
e. Not to accept favors or gifts from any user or other person potentially interested in gaining access to CCBC computing resources.
f. Not to do special favors for any user, member of management, friend, or any other person regarding access to CCBC computing resources in a manner that would circumvent prevailing security protections or standards.
g. Not to tell or disclose to any unauthorized person the information required to gain privileged access, or to engage in careless practices that would reveal that information to unauthorized persons.
h. Not to attempt to gain or use privileged access outside of assigned responsibilities, or beyond the time when such access is no longer required in job functions.
i. Not to change or develop any computer software in such a way that would (1) disclose computer information to unauthorized persons or (2) make it possible to retain any special access privilege, once that authorized privilege has been terminated by management.
j. Not to make arrangements on computer systems under their charge that will impair the security of other systems.
k. Not to modify or delete data unless it is done in accordance with CCBC policies and procedures.
l. To use all available protections to safeguard computer system(s) under their charge from unauthorized access by any person or another computer.
m. To report all suspicious requests, incidents, and situations regarding a CCBC computing resource to an appropriate member of management or the CIO.
n. To comply with all computer security standards and policies in force at the CCBC.

5.0 Sanctions

CCBC
The Community College of Baltimore County

Privileged Access and
Ethical Data Handling Agreement

Violation of the terms in this agreement will be dealt with seriously, and may subject the employee to loss of privileged access, and/or disciplinary action, including but not limited to termination. Illegal acts involving CCBC computing resources may also be subject to prosecution by all applicable federal, state, and local authorities.

I have read, understand, and agree to abide by the terms and conditions of this agreement.

_____
Employee Name (printed)

_____ _____
Employee Signature Date

_____ _____
Employee Supervisor Date