

BROWARD COMMUNITY COLLEGE
Information Technology
(Novell/Mainframe/Groupwise)
COMPUTER NETWORK SECURITY REQUEST FORM

Add User

A – User Information - Fill out options: A,B,C,D,&E

① Full Name: _____ SS# _____

② Title: _____ ③ Department: _____

④ Campus: Central Weston WHC North South Pines Ctr. Miramar/Automotive Overseas Ctr.

⑤ Location: (Bldg.#) _____ (Room#) _____ ⑥ Phone#: 954-201- _____ ⑦ Fax#: 954-201- _____

⑧ Job Title/Position: Full-Time Career Employee Part-Time Employee
 Full-Time Faculty Adjunct Faculty
 Outside Consultant Administrator

B – Novell/NDS Access for Student Workers (Access is needed to view pay stub)

- Yes, Creation of H: drive, Personal storage drive (**not** needed to view pay stub)
 Yes, Access to S: drive, College wide shared drive (**not** needed to view pay stub)
 Yes, Access to P: drive, Departmental drive (**not** needed to view pay stub)

C – Groupwise Email Access (Access is **not** needed to view online pay stub)

- Yes, Groupwise Access No, Groupwise Access

D – Faculty Web Page Access ******(Only full-time Faculty and adjuncts are eligible for personal web space)******

- Yes, I will require access to create/maintain my own personal web space on the BCC site.
 No, I will not require access to create/maintain my own personal web space on the BCC site.

E – Employee & Supervisor Authorization

User Signature: _____ Date: ____/____/____

Supervisor Signature: _____ Date: ____/____/____

Please Print Name: _____

Notes:

For special situations/circumstances:

Note: *Network User ID: will be the 1st initial of first name, plus seven characters of last name*

CID Access – To get CID access to specific areas/groups please print and fill out the form on the following link:
http://www.broward.edu/informationtechnology_57/SupportingContent/CID%20Campus%20User%20.pdf

Authorized Supervisor Signature Date: ____/____/____

*Keep a copy of this form for your records. **Send the completed and signed form to: Help Desk, DTC***

BROWARD COMMUNITY COLLEGE
Fair Use Guidelines & Security Rules & Affidavit

The College Computing Facilities, World Wide Web Site, and Email Accounts

The purpose of this agreement is to create an awareness of the rules of the college network and email system as defined in the College Policies and Procedures (6Hx2-8.01, 6Hx2-8.02, 6Hx2-8.03, 6Hx2-8.04, A6Hx2-8.01, A6Hx2-8.02, A6Hx2-8.03, A6Hx2-8.04). The following summarizes those policies and procedures, the complete documentation is available on www.broward.edu.

Fair Use Guides:

- 1) Use of the college network and email systems shall be based on college or academic need.
- 2) Employees are expected to check e-mail to ensure they are kept up-to-date on official college correspondence.
- 3) E-mail may not be used to impersonate another person or misrepresent authorization to act on the behalf of others or the college.
- 4) With the exception of academic reasons, Broward Community College prohibits employees from using the Internet to intentionally visit sites that are pornographic, sexually explicit, racially or ethnically biased or harassing or offensive in any way, either in graphic or text form.
- 5) The College will provide licensed software for College owned personal computers as part of a standard desktop configuration. Any additional software installed on a personal computer will be the responsibility of the Department or individual. Software may only be installed in strict accordance with the license agreement accompanying the software.
- 6) Only authorized Broward Community College employees or vendors will install software on College computers.
- 7) Computers that do not have active, approved virus detection shall not be connected to the College Network.
- 8) Users must not cancel automatic virus scanning or updating of definitions. If such automatic activity interferes with the user's duties, the user should contact the College Help Desk for additional support.
- 9) Broward Community College reserves the right to monitor any and all network and email activities to and from any computer directly connected to the College Network, including Internet access.
- 10) Each employee is assigned a user ID and password and is held responsible for all actions performed, and all data which is modified or retrieved under their user ID and password.
- 11) User IDs, accounts, or passwords may not be shared with another person under any circumstances.
- 12) The employee's job function and department requirements will determine the level of access to network directories and applications. Users can be provided access to other systems with written authorization from their supervisor and application data owner.
- 13) The following activities are **prohibited**:
 - Attempts to adversely affect the availability or quality of service of the Broward Community College Network.
 - Storing, posting, or displaying obscene or offensive data, even temporarily, in areas where someone might view them passively or inadvertently, except in cases where academically necessary.
 - Attempts to circumvent established security procedures or to obtain access privileges to which a user is not entitled.
 - Attempts to modify computer systems or software in any unauthorized manner.
 - Unauthorized access, alteration, or destruction of another user's data, programs, or electronic mail.
 - Attempts to obtain unauthorized access to either local or remote computer systems or networks.
 - Manipulation of others to gain information for the purpose of gaining access to commit fraud or damage to the system.
 - Using a program or procedure that looks like a normal logon process but instead records the user's password and user name.
 - Executing any form of network monitoring which will intercept data not intended for the user's host.
 - Attempting port scanning, network sniffing, packet spoofing, denial of service and forged routing information for malicious purposes.
 - Using any program, script, command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session.
 - Theft or destruction of computer hardware or software.
 - Any criminal activity or any conduct that violates applicable laws.

USER ACCEPTANCE:

By signing this form, I have read and I clearly understand my responsibility and will abide by the above terms and condition of the Fair Use Guide and Security User Rules for use of these facilities. I acknowledge receipt this date of a written copy of this form. If the propriety of any situation is unclear, I will ask for clarification from the System Administrators rather than making any assumptions.

Employee Signature

_____/_____/_____
Date

Printed Name

Dept Name

Campus/Bldg.#/Room

(954) 201 - _____
Phone#