

COMPUTER SECURITY

J-341.6 AR
(also E-630 AR)

College information technology resources are intended for use by BTC staff, students and customers (hereafter referred to as “computer users”). Authorized computer users will be provided a logon identification and temporary password at the time of initial employment or student registration. The network logon ID gives computer users access to BTC computer network services such as the Internet, Banner, email, Microsoft Office Suite and other software applications. BTC may override any password or pass code at any time in connection with its use of computer resources.

User names and passwords are unique to individuals. Once given access to College computing resources, staff and students are responsible for all use made of those resources under their user identification. User passwords, including personal, application and network passwords, must not be shared. Individual users shall be held accountable for incidents related to unauthorized use of their password or incidents related to sharing a password. Passwords are to be kept confidential and known only by the assigned user. Passwords should be changed frequently as an additional protective measure. Passwords or passphrases must be complex, meaning that they contain upper case, lower case, symbols, and numbers, or at least three of those four groups, and must be eight characters or longer. Computer users will be prompted every 180 days to change their password.

When logged onto the BTC computer network, computer users are responsible for ensuring the security of the computer resources, including never providing access to unauthorized users and ensuring that workstations are not left unsecured; employees and students are encouraged to lock their workstation or logoff when they are not present.

Computer users with passwords and network authority must not use this privilege to gain access to any workstation, server or user folders beyond that which is specifically associated with assigned work responsibilities or student coursework. Network access and directory/files security management will be centralized in Information Technology Services (ITS) and Management Information Systems (MIS).

Computer users shall not encrypt files or take other steps to block access to files unless specifically required to protect confidential or sensitive information related to a BTC activity or requirement.

Computer users shall not probe, scan, capture data, or test security. Unauthorized possession or use of special tools for cracking security is prohibited.

Computer users may not install personal security software or password protection schemes that prevent ITS technicians from accessing installed software on the network or on local machines. BTC uses a centralized application deployment system to maintain college-supported software

COMPUTER SECURITY

J-341.6 AR
(also E-630 AR)

and operating systems. Any software or hardware that prevents these automated systems from assessing a workstation will be removed which may include re-imaging the computer.

Staff and students should immediately report any security vulnerabilities or other potentially dangerous situations to the Chief Information Officer.

Reference: District Board Policy C-200 Employee Code of Ethics
District Board Policy J-341 Student Code of Conduct

Administrative Regulation Adopted: March 29, 2004
Revised: February 4, 2008; May 24, 2010