
IT Security Standard:

Security Privileges

Introduction

This standard defines the steps needed to implement the Bellevue Community College (BCC) IT Security Policy within the context of varying levels of user security privileges on various systems. The necessity of this standard is to assure the integrity and reliability of the BCC internal networks and the computers on those networks. The standard will be reviewed on an annual basis or when changes are implemented.

Scope

This standard defines the security privileges granted to BCC users and the specific procedures for granting administrative privileges to BCC networks and computing systems.

Exceptions

A variety of exceptions to this standard may be expected. These exceptions, when granted, will be documented in either a platform specific standard or in a memo documenting the exception. Exceptions may be granted by the BCC IT Security Administrator, the Dean of Information Resources (IR), or any IR director authorized by the Dean. Copies of all documentation regarding exceptions will be kept on file with the BCC IT Security Administrator. This documentation will include:

1. A detailed description of the exception.
2. A description of why the exception is necessary.
3. A risk assessment by the BCC IT Security Administrator and/or the Dean of Information Resources, or designee.
4. A description of the compensating controls that are in place to mitigate risk created by the exception.

Business Impact and Risk, Threat, and Vulnerability Analysis

Authorized BCC support personnel will have total administrative privileges on all the networks and computing systems used at BCC. These personnel are trained and carefully supervised to handle this necessary aspect of technology support on campus. However, standard campus users generally have neither the training, nor the understanding of security issues or network integrity. As such, judiciously granting administrative privileges, even only to local systems, becomes a critical factor in assuring the security of the computing and communications resources under BCC's responsibility. Any misuse of these security privileges could put the college instructional and business systems at great risk.

Given the high level of access inherent in administrative privileges to BCC systems, the most significant threats are:

1. Malicious and/or unauthorized access to data
2. Malicious and/or unauthorized modification of data
3. Accidental modification of data (e.g., while performing support)
4. Theft of equipment or resources
5. Malicious and/or accidental damage to equipment or resources
6. Malicious and/or accidental denial/loss of service

Given the nature of the asset and the nature of the threat, all risks associated with granting users administrative privileges are very significant, and could cause significant loss to BCC.

Standard

Security Privileges

BCC users are granted standard security privileges or access to the computing equipment assigned to them sufficient to perform their official duties. System administration, installation and removal of software (including plug-ins and system patches), and repair of BCC systems are the principal responsibilities of authorized BCC IR support personnel or authorized designees.

In some circumstances—including physical distance of the system from BCC, special technical needs, and research and development—it may become necessary for the user of a BCC-owned computer to perform some of these tasks. This may include, but is not limited to, such things as: updating patches, installation and removal of software, file system backups, server administration, and other related tasks. In these cases, BCC employees will be granted local administrative privileges for the specific computing system assigned to them.

To be granted these increased local administrative privileges, the BCC Computer Administrative Privileges Agreement (Appendix B) will be completed and signed by the individual and the immediate supervisor.

Local Administrative Privileges Guidelines

Any administrative privileges authorized to individual users will only be “local” in nature. This means they will be given full rights and control to read, write, and modify any files only on the specific computer for which they have been granted these rights. They will also be able to execute all program files and list all folder contents.

Those granted local administrative privileges on a BCC-owned computer will adhere to the following guidelines at all times:

1. Administrative privileges to any BCC network resource will be strictly restricted to authorized BCC technical support personnel, or authorized designee.
2. Users who have authorized administrative privileges will be in compliance with this standard and all applicable BCC policies at all times.
3. Authorized users will exercise due care and caution to ensure the integrity of all BCC networking and computing systems.
4. Any users granted administrative privileges are expected to review and fully abide by all applicable copyright and licensing policies. These include, but may not be limited to: BCC’s policies on the Acceptable Use of State Resources, on the Acceptable Use of the BCC Network and BCC Data Management Systems, on the Acceptable Use of BCC Computers, the BCC IT Security Policy, the BCC Software Licensing Compliance Policy, any CIS and/or DIS software copyright policy, and state and/or federal law.
5. A user with elevated security privileges will not install software on any BCC-owned computer without having provided to Computing Services the appropriate proof of ownership as spelled out in the IT Security Standard addressing “Software Management.”
6. Under no conditions may anyone granted administrative privileges under this agreement remove, alter, or reconfigure any software that has been installed by BCC IT support personnel to assist in monitoring and/or support of any BCC-owned computer.
7. The user is expected to review and abide by all BCC IT security policies and standards.
8. If the circumstances for which the user requires administrative privileges change, that user will notify IR that the administrative privileges are no longer required.

Remedies

These administrative security privileges will be revoked, without warning, if it appears there has been a deliberate attempt by the user to elevate privileges, or to utilize privileges to gain unauthorized access to BCC networks or systems to which access authorization has not been given.

1. The suspected breach of security will immediately be reported to the Dean of IR or authorized designee, to the BCC IT Security Administrator, and to an appropriate unit administrator.
2. The breach will be investigated in accordance with the procedures identified in the Acceptable Use of the BCC Network and BCC Data Management Systems Policy, and the BCC IT Security Standard addressing "Intrusion Detection and Incident Response."
 - a. If the suspected breach of security is determined to be unfounded, the user's administrative privileges will be restored as soon as possible
 - b. Validated deliberate breaches of security will be reported to the Dean of Information Resources and to the individual's immediate supervisor for appropriate action. Human Resources will be notified, as appropriate.
 - i. Appropriate disciplinary procedures in accordance with BCC policies and procedures will take place, as needed.
3. If a workstation for which administrative security privileges have been granted under this standard is determined to be compromised in any way or is determined to be the cause of problems on any BCC network, Information Resources technical support staff will take appropriate corrective steps.
 - a. This will include disconnection of the workstation from all BCC resources immediately and without warning. Every attempt will be made to notify the workstation owner and the immediate supervisor in advance of this action.
 - b. There will be a request for a specific cleanup procedure, up to and including a request to allow technical support to reinstall the OS.
4. Administrative security privileges will be revoked at any time if the issues identified by Information Resources technical support personnel are not addressed by the workstation owner in the requested manner.
5. Information Resources technical support personnel will set the hard drive image back to default and reassign privileges to the campus standard.
6. The owner's account(s) will be disabled and network connectivity will be discontinued until the workstation is reconfigured as necessary or removed from the network.

Review

All administrative privileges granted under this standard will be reviewed annually by the BCC IT Security Administrator or authorized designee.

1. A copy of the approved form will be kept on file by the BCC IT Security Administrator.
2. The user will be notified by IR as soon as possible of any changes in their security privileges related to this agreement.

Staff Separation

As explained in the BCC IT Security Standard addressing "Password Management", all account access and administrative privileges granted under this standard will be disabled on an employee's last day of employment. Human Resources will be advised when this has been done.

1. The Director or Organizational Unit Administrator (OUA) to whom the person reported may choose to have some, or all, administrative access disabled prior to the actual separation date.
2. The Director or OUA to whom the person reported is responsible for informing Information Resources of the employee's separation no later than when it occurs (i.e., the employee's last day in the office).

Sanctions

Violations of the provisions of this, or any BCC IT security standard or policy, will be dealt with immediately in the same manner as any violations of BCC policies, and may result in disciplinary review. In such a review, the full range of disciplinary sanctions is available, including:

1. Permanent loss of computer use privileges;
2. Denial of future access to BCC IT resources;
3. Disciplinary action – any disciplinary action will be taken in accordance with appropriate procedures as established by the Vice President of Human Resources (for employees) or the Dean of Student Services (for students);
4. Dismissal from the college; and/or
5. Legal action.

Those users who misuse or abuse any computing or network resource may have their login accounts closed and access to the systems immediately terminated. Some violations of this standard may also constitute a state, local, or federal criminal offense.

Appendix A – References

1. BCC Acceptable Use of State Resources Policy
2. BCC Acceptable Use of the BCC Network and BCC Data Management Systems Policy
3. BCC Acceptable Use of BCC Computers Policy
4. BCC IT Security Standard: Intrusion Detection and Incident Response
5. BCC IT Security Standard: Password Management
6. BCC IT Security Standard: Software Management

Effective Date: July 2003
Date Last Modified: July 21, 2006

(Versioning: will be removed upon final approval of updates.)

Date	By	Notes
July 2003	Farris	Final
May 2004	Farris	Update
July 2004	Farris	Update to Admin Privileges Form
July 2006	Farris	Updated with Exceptions and Sanctions language, and for style requirements.

Appendix B –



3000 Landerholm Circle SE, Bellevue, WA 98007-6484 | www.bcc.ctc.edu

BCC Computer Administrative Privileges Agreement Form

This form will be completed and signed before any BCC employee will be granted local administrative privileges on any BCC-owned computing equipment whether that computer is attached to the BCC internal network or is set up in a stand-alone configuration.

Introduction

As a general principle, campus users are granted privileges or access to the computing equipment assigned to them sufficient to perform their job duties. System administration, installation and removal of software (including plug-ins and system patches), and repair of BCC systems is the principal responsibility of authorized BCC IR support personnel.

In some circumstances—including physical distance of the system from BCC, special technical needs, and research and development—it may become necessary for the user of a BCC computer to perform some of these tasks. This may include, but is not limited to, such things as: updating patches, installation and removal of software, file system backups, server administration and other related tasks. In these cases, the BCC employee will be granted “local” administrative privileges for the specific computing system assigned. This means they will be given full rights and control to read, write, and modify any files only on the specific computer for which rights have been granted. The employee will also be able to execute all program files and list all folder contents.

Any BCC employee needing local administrative privileges will request it in writing using this form. Authorized users granted administrative privileges on a BCC-owned computer will at all time follow the guidelines explained in the BCC IT Security Standard for Security Privileges, which defines the expectations for, and requirements of, such privileges. This agreement will be signed by the individual, the immediate supervisor and the appropriate IR representative before such privileged access is granted.

Compliance with the standard will assure the integrity and reliability of the BCC internal networks. It is further extended to computers not directly attached to the BCC network, but which are owned by BCC, so as to protect these valuable resources from misuse and/or accidental damage.

Requirements

Any administrative privileges authorized to the individual user will only be local in nature. Administrative privileges to any BCC network resource will be strictly restricted to authorized BCC technical support personnel.

Authorized users share the following responsibilities, and must be able to certify to BCC technical support staff, at any time, that they are in compliance:

1. The authorized user will exercise due care and caution to ensure the integrity of the system.
2. The user is expected to review and abide by all applicable copyright and licensing policies. These include, but may not be limited to: BCC’s IT Security Policy, BCC Software Licensing Compliance Policy, any CIS and/or DIS software copyright policy, and state and/or federal law.
3. The user is expected to review and abide by all applicable BCC acceptable use policies.
4. The user is expected to review and abide by all BCC IT Security Policies and Standards.
5. The user may not install software without being in compliance with the expectations of the BCC Software Licensing Compliance Policy. This includes providing appropriate software copies and licensing information to Information Resources.

6. If the circumstances for which the user requires administrative privileges change, the user will notify IR via Request Center that the administrative privileges and privileges are no longer required.
7. These administrative privileges will be revoked, without warning, if it appears there has been a deliberate attempt by the user to elevate privileges or to utilize their privileges to gain access to BCC networks or systems to which access has not been authorized.
 - a. The suspected breach of security will immediately be reported to the Dean of Information Resources or designee, the BCC IT Security Administrator, and to an appropriate administrator representing the user's unit.
 - b. The breach will be investigated in accordance with the procedures identified in the Acceptable Use of the BCC Network and Data Management Systems, and the BCC IT Security Standard addressing "Intrusion Detection and Incident Response."
 - i. If the suspected breach of security is determined to be unfounded, the user's administrative privileges will be restored as soon as possible
 - ii. Validated deliberate breaches of security will be reported, for appropriate action, to the Dean of Information Resources and to the Administrator to whom the individual reports.
8. If a workstation for which administrative privileges have been granted under this standard is determined to be compromised in any way, or determined to be the cause of problems on any BCC network, BCC technical support staff will take appropriate corrective steps.
 - a. This will include disconnection of the workstation from all BCC resources immediately and without warning. Every attempt will be made to notify the workstation owner and the immediate supervisor in advance of this action.
 - b. This will be a request for a specific cleanup procedure, up to and including a request to allow technical support staff to reinstall the OS.
 - c. If necessary, designated Information Resources technical support staff will set the hard drive image back to default and reassign rights to the campus standard.
9. Administrative security privileges will be revoked at any time if the issues identified by BCC technical support personnel are not addressed by the workstation owner in the requested manner.
10. The owner's account(s) will be disabled and network connectivity will be discontinued until the workstation is reconfigured as necessary or removed from the network.
11. All administrative privileges granted under this standard will be reviewed annually by the BCC IT Security Administrator or authorized designee.
12. A copy of the approved form will be kept on file by the BCC IT Security Administrator.
13. The user will be notified by IR as soon as possible of any changes in security privileges related to this agreement.

I understand and agree to abide by the BCC IT Security Standard addressing "Security Privileges." I affirm I have reviewed the other BCC policies and procedures specified in this document. I understand all security privileges granted in conjunction with this request will be reviewed annually. I acknowledge that I have received a copy of this form.

Reason for requesting local administrative privileges:

Description of system for which privileges are being requested:

Printed Name

Date

Signature

Supervisor Approval (Signature)

Date

IR Approval (Signature)

Date

Date Review Due