575.1 — PURPOSE

Computers at Bridgerland Applied Technology College (BATC), which are connected to the Internet, are at risk of being compromised as a result of unauthorized access into resources and confidential data stored on, or transmitted through, the BATC network. Data housed on the network must be protected from security breaches, vulnerabilities, and loss. The purpose of this procedure is to protect the security and prevent the loss of information that is critical to the operation of BATC.

575.2 — DEFINITIONS

Chief Information Officer (CIO): BATC's Chief Information Officer provides direction and ongoing analysis and planning of the LAN/WAN, directing decisions for changes, upgrades, and new projects to facilitate the changing needs of BATC.

Compromise: A vulnerability that has been found and exploited by an unauthorized user.

Critical Institutional Data (CID): Any information that is generated or acquired, stored, and required for the continued function of BATC, including, but not limited to: academic records, employment records, financial records, schedules, etc. CID is owned by BATC (except for information that is PSI, see below).

Information Systems Resource (IS Resource): A resource used for electronic storage, processing, or transmitting of any data or information, as well as the data or information itself. This includes, but is not limited to, electronic mail, local databases, externally accessed databases, CD-ROM, recorded magnetic media, photographs, digitized information, or microfilm. This also includes any wire, radio, electromagnetic, photo optical, photo electronic or other facility used in transmitting electronic communications, and any computer facilities or related electronic equipment that electronically stores such communications.

LAN: Local Area Network is a computer network that connects computers and devices in a limited geographic area, such as a school.

Network Administrator: BATC staff, under the direction of the CIO, has day-to-day operational responsibility for data capture, maintenance and dissemination; and is charged with the responsibility of managing and maintaining the campus network and other systems and resources.

Network Scanning: Any systematic attempt to communicate with a class of network addresses via a particular port or protocol to ascertain which computers respond (a first step to identify and exploit vulnerabilities).

Network Traffic Patterns: Information about the source, destination, protocol, port, and bandwidth of network packets.

Private Sensitive Information (PSI): Any information that might result in a loss to its owner if the information was obtained by someone with unknown trustability or malicious intent. PSI includes, but is not limited to, the owner's name combined with: social security number, birth date, access passcodes, academic record, medical history, and/or financial matters. PSI is owned by the named individual, not BATC.

Server: A computer used to provide information and/or services to multiple users.

Vulnerability: Lack of a security barrier to unauthorized access or use.

WAN: Wide Area Network is a computer network that covers a broad area.

575.3 — POLICY STATEMENT

BATC must take measures to protect PSI and CID that are housed, processed, or transmitted using BATC resources. All computers and other IS Resources utilized to display, process, store, or transmit PSI or CID must be maintained solely by BATC's IS personnel.

575.4 — ROLES AND RESPONSIBILITIES

The **CIO** provides leadership in the management and application of educational information and CID for BATC. The CIO ensures that instructional information management and technology systems are integrated, provides ongoing analysis and planning of LAN/WAN operations, directing decisions for changes, upgrades, and new projects to facilitate the changing needs of BATC.

The **Network Administrator** provides technical and administrative support for the network. The Network Administrator installs, upgrades, and maintains the network infrastructure; maintains adequate knowledge of existing hardware and software in use to maximize efficiency of the network and users' utilization of them and provides written documents which evaluate network information on periodic intervals.

575.5— BACKUP PROCEDURES

AS/400
No backup after Feb 2013. No new data entered. Complete backups are stored both on-site and off-site.

All server backups are done on an ~~Eversync~~ Infrascale/Eversync disc array appliance.

Contents:

Admin	E:, F:, G:, H:
AMS_SQL	*all SQL databases
APPS	E:\BMI, F:, G:
APPS_SQL	*all SQL databases
BCC1	E:, F:, G:
BUS	E:, F:, G:
~~Dentrix~~	~~C:\Program Files\Dentrix\Data~~ ~~C:\Program Files\Dentrix\Doc~~ ~~C:\Click8\~~ ~~C:\Dexis\Data~~
Dept	E:, F:, G:
DLS	C:\Kaba, SQL
Draft2	E:, F:, G:, H:
ISC	System State
ISP	C:, System State
JDBS	C:, D:, E:, F:, G:, System State, Live BMR
JDBS_SQL	*all SQL databases
JWEB	C:\inetpub. D: (VSS)
TEI	V:

Backup Scheme:
Full backup on the 1st Monday of each month at 10:00 p.m.
Differential backup each Saturday at 10:00 p.m.

Incremental backup each Monday through Friday at 10:00 p.m.
*SQL databases - full backup each Monday through Saturday
Archive tape changed on the 1st Monday morning of each month

Backups are retained as follows:

- Full backups – 6 months
- Differential backups – 1 month
- Incremental backups – 14 days
- Archive drive – rotated monthly with a set of two drives. Contains all backups for one month period. Inactive drive is stored off-site.

A log file of all backups is maintained at ADMIN/vol1:is\backuplog\tapelog.xls and also on the IS Manager's local hard drive C:\data\excel\tapelog.xls

575.6 — DISASTER RECOVERY PROCEDURE

In the event of a disaster at Bridgerland Applied Technology College that results in loss of data processing equipment or the data that it contains, the following procedures outline methods to recover the data and access to it. This document will address total loss of equipment and data. Obviously, only the portions of this document that apply to the equipment/data lost need to be addressed.

1. Obtain and replace any defective equipment (see list of vendors below)
2. Connect/configure network hardware as required
3. Load Operating System/software as required
4. Restore data from backup appliance (see Backup Procedure document-attached)
5. Contact technical support as required (see list of support vendors below)

Servers:
~~*Accounting system* - IBM AS/400 model 9402~~
~~*Disk space* - 7 gig~~
~~*Operating system* - OS400 V3R2~~

- AS/400 Computer
- ADMIN server
- AMS server
- APPS server
- BCC1 server
- BUS server
- ~~DENTRIX server~~
- DEPT server
- DLS server
- DRAFT2 server
- ISC server
- ISP server
- JDBS server
- JTS server
- JWEB server
- TEI server
- ELearn Streaming Server

Network hardware:

- Cisco 3750 switch
- Cisco 3550 switch
- Cisco 3550G switch
- Cisco 2970 switch
- Cisco 2960 switch
- Cisco 2950 switch
- Cisco ASA 5250 firewall
- Cisco PIX 515 firewall
- Cisco 5508 Wireless Controller

**Note: a copy of all Cisco configuration files are on the off-site backup archive drive (\\admin\IS$\ciscobackupfiles).
~~8e6 R3000 content filter~~ iBoss model 14500 content filler

Support contacts:

IBM	hardware support	IBM 800-426-7378
		AMX 949-675-3147
	software support	AMX 949-675-3147
Hewlett-Packard	hardware support	Valcom 801-262-9277 Ken
	hardware vendor	Valcom 801-774-0527 Jeff
Eversync backup	total support	Eversync 801-263-5116
~~*8e6*~~	~~hardware support~~	~~8e6 888-786-7999~~
iBoss	hardware support	858-568-7051 ext. 3
Cisco	hardware support	Cache Valley Electric 801-631-5330 John

575.7 — SERVER AND INFORMATION SECURITY, NETWORK MONITORING, AND VULNERABILITY SCANNING

- Servers housed at BATC are located behind secure doors, with limited access.
- Hardware and software firewalls are configured to block access to the Intranet from the outside. Antivirus and antispyware software is used on all BATC servers and workstations.
- Users are required to change their password every 90 days and must maintain at least two passwords.
- The Utah Education Network (UEN) monitors network traffic patterns and probes ports of computers by conducting networking scanning for the purpose of identifying vulnerable and compromised computers on the BATC network. This monitoring occurs 24 hours per day, 7 days per week, and 365 days per year. All computers and communications devices connected to the BATC network are subject to this monitoring. Vulnerabilities or compromised machines are identified and e-mail notifications are sent to both the BATC CIO and Network Administrator daily. Compromises and other security breaches are resolved immediately to protect the network resources.

575.8 — RISK MITIGATION

BATC stores a large amount of data (both digital and hard copy), which includes personal, non-personal, sensitive, and confidential information. Care should be taken to protect this data to ensure that it is not changed (either accidentally or deliberately), lost, or stolen. Data breach insurance is being pursued through State Risk Management for protection in the event of a data breach. If State Risk Management doesn't offer insurance options, other arrangements will be made.

575.9~~8~~ — ACCEPTABLE COMPUTER USE GUIDELINES AND PROCEDURES

All computers at BATC are shared educational resources of the State of Utah for the primary use of professional staff and student access. The use of the network and/or online courses is considered to be a privilege and is permitted to the extent that available resources allow. With this privilege come certain responsibilities that need to be understood and carried out by all users. Classroom computer settings must remain constant to provide a quality training environment for all users. **Therefore, any student found adding, modifying, or deleting current computer settings or software (i.e., screen savers, wallpaper, graphics, games, unlicensed software, instant messaging client, file sharing, downloading of copyrighted materials, etc.) will be subject to appropriate disciplinary action and possible termination from BATC.**

BATC **does not** provide e-mail accounts for students.

Users must accept the responsibility of adhering to high standards of professional conduct and act in a responsible, decent, ethical, and polite manner. Internet use is for the purpose of encouraging the pursuit of higher knowledge. Although reasonable effort is made to filter out controversial material, each individual's judgment regarding appropriate conduct in maintaining a quality resource system is essential. Students will treat their instructors, fellow students, and support staff with respect both in the physical and online classroom environments.

While this does not attempt to articulate all required behavior by its members, it does seek to assist by providing the following guidelines:

1. All use of the Internet must be in support of a world class public education and educational research in Utah and consistent with the purposes of the network.

2. Computer accounts shall be used only by the authorized owner of the account. Account owners are ultimately responsible for all activity under their account. All communications and information accessible via the Internet should be assumed to be private property. Great care is taken by the network's administrators to ensure the right of privacy of users. However, it is recommended that users not give out personal information like home addresses and/or telephone numbers. Also, passwords should be kept private and changed frequently.

3. No personal laptop computers, desktop computers, smart phones, tablet devices, or any other personal device capable of network connection will be allowed on the BATC network; although, personal devices may connect to the Internet via BATC's wireless network. Personal network devices such as wireless access points, routers, servers, firewalls, etc., are not allowed.

4. Prohibited behaviors include:
   - Sending or displaying intimidating, offensive, or inappropriate messages or pictures
   - Illegal activities (defined as a violation of local, state, and/or federal laws)
   - Harassing, insulting, or attacking others
   - Using another person's password/account
   - Accessing another person's computer, folders, work, or files without their consent
   - Possessing or using any software tools designed for probing, monitoring, or breaching the security of a network
   - Violating copyright laws
   - Having someone else complete work
   - Using additional materials to complete exams
   - Any use for commercial purposes or financial gain
   - Any use for product advertisement or political lobbying
   - Any use which shall serve to disrupt the use of the network by other users
   - Extensive use of the network for private or personal business

5. In regard to e-mail, chat rooms, and threaded discussions (if applicable), "netiquette" includes:
   - Having appropriate e-mail addresses
   - Using only language that would be appropriate in any face-to-face classroom at BATC
   - Respecting the comments of teachers and other students. Discussions and disagreements over issues are appropriate; however, put-downs or any type of negative comments about another student or instructor is not appropriate

6. This is a legally binding document and careful consideration should be given to the principles outlined herein. Violations of the provisions stated in this document may result in suspension, revocation of network privileges, and/or dismissal/termination.

7. The above-mentioned use is subject to revision.

As necessary, BATC will determine whether specific uses of the Internet are consistent with this document. BATC shall be the final authority on use of the network and the issuance of user accounts.

575.10~~9~~ — TECHNOLOGY PROTECTION MEASURE

An internet filtering device is in place and functioning at all times that blocks or filters internet access by all users to obscene and/or pornographic materials. This device also monitors internet activity of users.

575. 11~~10~~ — INTERNET SAFETY

BATC does not allow minors access to inappropriate and objectionable internet materials and prohibits access to unlawful and harmful online activities. Access to personal information of minors is restricted.

BATC hosts minor age students from local area high schools for a portion of the school day and assumes that proper education about appropriate online behavior, including cyberbullying awareness and interacting on social networking sites and chatrooms, is being conducted, as required by law, at those high schools.

BATC Staff/Student Application for Computer Use

Students may be allowed use provided they read and sign thus agreeing to follow all guidelines; obtain one teacher's signature (if a student), who will act as sponsor; and obtain the signature of a parent, if under age 18.

Applicant _____ Staff/Student (please circle one)

School Bridgerland Applied Technology College

Address 1301 North 600 West, Logan, UT 84321 Phone _____

I have read the BATC Acceptable Computer Use document and agree to abide by its provisions. I understand violation of the use provisions stated in the document may constitute suspension or revocation of network privileges.

Signature _____ Date _____

Sponsoring Teacher(s) (required for students)

I agree to sponsor the above student and to supervise his/her responsible use of the network as defined by the BATC Acceptable Computer Use document while in my classes.

Teacher's Signature _____ Date _____

Sponsoring Parent or Guardian (required for students under 18)

I have read the BATC Acceptable Computer Use document. I understand administrators of the network have taken reasonable precautions to ensure that controversial material is eliminated on BATC's Network. I hereby give my permission to issue an account for my child and certify that the information contained on this form is correct.

Parent's or Guardian's Signature _____ Date _____

Address _____ Phone _____

BATC Approved by _____ Date _____