BALTIMORE CITY COMMUNITY COLLEGE

INFORMATION TECHNOLOGY SECURITY PLAN

FEBRUARY 2011

TABLE OF CONTENTS

DEFINITION

Confidentiality - "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" and "A loss of confidentiality is the unauthorized disclosure of information." (*DOIT 2009: Information Security Policy*)

Integrity - "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity ..." and "A loss of integrity is the unauthorized modification or destruction of information." (*DOIT 2009: Information Security Policy*)

Availability - "Ensuring timely and reliable access to and use of information…" and "A loss of availability is the disruption of access to or use of information or an information system." (*DOIT 2009: Information Security Policy*)

Information Technology Resources - includes all college-owned computers, applications software, systems software, databases, and peripheral equipment; the data communications infrastructure; the voice communications infrastructure; communication services and devices, including electronic mail, voice modems, and multimedia equipment. The components may be stand-alone or networked and may be single-user or multi-user systems.

Information Security Event - any situation that has the potential to threaten the confidentiality, integrity, and availability of the College's information and information technology resources. An event includes loss of control of information through unauthorized access, equipment loss, or theft.

Information Security Incident - any event that is known or suspected to have compromised the confidentiality, integrity, and availability of the College's information and information technology resources.

Breach - the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to events where persons other than authorized users have access or potential access to confidential or sensitive information, either electronically or physically.

CITS – the Computer Information Technology Services Department.

CITO – the Chief Technology Information Officer in CITS.

ITRT – the Information Technology Response Team which comprises of IT professionals assembled to address a breach or information security event or incident.

PURPOSE

This Information Technology Security Plan describes Baltimore City Community College's safeguards to protect the confidentiality, integrity, and availability of information and information technology resources. This plan is in compliance with the State of Maryland's Department of Information Technology (DOIT), Information Security Policy, Version 2.2. Also, this plan is in compliance with provisions of the Gramm-Leach-Bliley Act of 1999 regarding the Safeguards Rule of customer records, and the privacy rules of the Family Educational Rights and Privacy Act (FERPA).

SCOPE

This Information Technology Security Plan applies to all College information that is electronically generated, received, stored, typed, copied, and printed. The provisions of this plan apply to activities, methodologies, and procedures implemented by the Computer Information Technology Services (CITS) Department to protect all College information. The scope of this plan specifically focuses on the following areas:

- IT Security Policy
- Risk Management Process
- IT Incident Response Process
- IT Disaster Recovery Plan
- Security Awareness

INTRODUCTION

Innovations in digital technologies have rapidly increased the use of information technologies in all facets of college life. With that said, information and information systems are considered vital assets to our institution, providing essential services to our students, faculty, and staff. Therefore, it is crucial for colleges to establish precautions to protect its information from unauthorized access, modification, disclosure, and destruction.

The State of Maryland Department of Information Technology, Information Security Policy prescribes a set of minimum security requirements necessary to protect the confidentiality, integrity, and availability of State-owned information. Baltimore City Community College (BCCC), an agency of the State of Maryland, is mandated to carry-out those security requirements. Thus, all information generated, received, stored, typed, copied, and printed with BCCC's resources for the purpose of conducting college-related business is considered State property and is protected under the provisions of this Information Technology Security Plan.

Note: The State acknowledges that Not All components of their Information Security Policy would be applicable to some agency (***DOIT 2009: Information Security Policy, Section 4***.) Therefore, as BCCC is also an educational institution, some components of the State's policy are not applicable.

SECTION 1: IT Security Policy

It is the policy of Baltimore City Community College to implement and maintain an Information Technology Security Plan that protects the confidentiality, integrity, and availability of information. Specifically, the plan provides safeguards to: (a) ensure the security and confidentiality of students' and employees' records and sensitive information; (b) protect against potential threats or vulnerabilities to the security or reliability of students' and employees' records and sensitive information; and (c) protect against unauthorized access to or use of students' and employees' records and sensitive information. This plan is enforced through IT best practices and the College's policies, procedures, and standard operating procedures.

SECTION 2: Risk Management Process

Baltimore City Community College (BCCC) performs risk assessments on critical IT systems. This task is performed by the Network Administrators and the Security Infrastructure Officer during system implementation, scheduled replacement, and update cycles. Also, risk assessment is performed by the external auditors. The College recognizes that the risk of unauthorized use of information or access to information is probable. These risks include but are not limited to:

- Unauthorized access of information by an individual not considered the owner of the information;
- Compromised system security due to system access by an unauthorized individual;
- Interception of data during transmission;
- Loss of data integrity;
- Physical loss of data in a disaster ;
- Errors introduced into the system;
- Corruption of data or systems;
- Unauthorized access of information by employees ;
- Unauthorized requests for information;
- Unauthorized access through paper (hardcopy) documents;
- Unauthorized transfer of information through a third-party.

BCCC acknowledges that the above list of potential risks associated with the protection of information is not exhaustive. Notably, new risks of unauthorized use or access to information are created regularly due to the rapid advances in technology. However, the Computer Information Technology Services Department (CITS) will actively participate and monitor advisory groups such as the EDUCAUSE Security Institute, the Internet2 Security Working Group, the SysAdmin, Audit, Network, Security (SANS) Institute for identification of new risks to safeguard the college's information, and the Federal National Institute of Standards (NIST) Computer Security Resource Center.

2.0 Administrative Safeguards

Access to information from any of Baltimore City Community College's (BCCC) computer information systems are limited to employees who have a legitimate business reason to such information. Databases containing personal and sensitive information including but not limited to, students' accounts, balances, grades, financial records, employees' records and confidential information are available only to BCCC's employees in appropriate departments and positions. Each employee is given an account and password after receipt of documentation from a College official with the appropriate signatures has been received by the Computer Information Technology Services Department (CITS). Each student is given an account with the level of access to their email account and course information via the College's Student Portal and the Course Information System. Student access is restricted from any information system or information technical resource that is considered "Administrative." CITS will continue to take appropriate measures that are consistent with existing technological developments to ensure that all College information is secure, and to safeguard the confidentiality, integrity, and availability of information and information technology resources.

2.1 Operational Safeguards

The operational safeguards address security controls that are implemented on information systems. These controls help to enhance the security of the College's information and information technology resources. The controls are put in place by the professional staff in the Computer Information Technology Services Department (CITS), and enforced through policy, procedures, and standard operating procedures.

2.2 Access Controls

All "administrative" accounts require a valid user name and password in order obtain access to any College information and information technology resource. Authentication (logon process) will not occur without the above requirement. All system users will adhere to the minimum acceptable Password Standard (referenced in the *CITS Policies and Procedures Manual* and *the BCCC Center*), and described below:

- Password History = 3;
- Maximum Password Age = 90 days;
- Minimum Password Age = 5 days;
- Minimum Password Length = 8 characters;
- Password Complexity = minimum of 1 lower case, 1 upper case, 1 numeral or special character;
- Account Lockout Policy = 3 failed attempts.

In addition to the above-mentioned controls, access to critical systems is further enforced through the following standard operating procedures (referenced in the *CITS Policies and Procedures Manual* and *the BCCC Center*):

- Applications and Data Security Support Checklist for HP Logon Accounts;

- HP Access;
- HP User Access Entitlement Review;
- ADPIC – New User Access;
- FMIS User Access Entitlement Review;
- ADPIC – Termination of User Access.

2.3 Network Controls

Access to any network-connected computer must be via a logon process that identifies and authenticates the user, except where read-only access is given to a certain system, such as the library catalog, or unprivileged access is normal and the appropriate safeguard is in place, such as guest/public access in the Open Computer Labs. Also, computers configured with the whole or partial purpose of accepting connections from and exchanging information between other computers are defined by this plan as a server. The following controls apply to networked computers and servers:

- Servers must be located in secure areas with physical access controls such as keys, access cards, and or alarms. Unauthorized users who require physical access to a serve, or require access in the vicinity of a server, must be escorted by an authorized systems administrator;
- Servers must be located in an area that has the appropriated environmental controls, including air handling and conditioning, uninterruptible power protection (UPS) and conditioning, and fire suppression;
- Servers must be appropriately managed and monitored on a daily basis by an authorized systems administrator;
- Only an authorized systems administrator may modify a computer's network settings and parameters;
- Share accounts are not created.

2.4 Independent Network Controls

Independent Networks are systems connected to the college's IT infrastructure, but are not managed by the Computer Information Technology Services Department (CITS). These networks include the State's Financial Management Information System (FMIS), the Police Department Access Control Surveillance System, the Internet, Blackboard, and PayPal. The owners and users of independent networks are required to comply with the College's policies, procedures, and standard operating procedures, including the safeguards described in this security plan. Some of the safeguards pertinent to this plan include, but are not limited to:

- Agencies or departments hosting an independent network within the College must designate a qualified "Network Administrator" who will be responsible for devices connected within the independent network;

- A professional staff in CITS shall configure firewalls and routers' Access Control Lists (ACLs) to restrict the types of traffic that may be allowed to enter and leave the College's network infrastructure;
- All independent networks that have the capability to bypass the College's firewalls and ACLs must be approved and registered with CITS prior to being connected the College's network infrastructure. These independent networks include technologies associated with dialup access, wireless access, and Virtual Private Networks (VPNs);
- All devices associated with independent networks shall be monitored and scanned to detect potential threats or a security breach. If a breach is perceived, the Information Security Officer will be notified immediately. In the event, the Information Security Officer is unavailable; a Network Administrator will disconnect that device(s) from the College's network infrastructure;
- Independent networks are required to display Baltimore City Community College's IT Security Policy displayed or referenced in a banner when users logon to the systems.

2.5 Wireless Controls

The airwaves local to the Baltimore City Community College's campuses are considered a transmission medium, whereby voice and data communications are prevalent. As the airwaves are a shared resource, the Computer Information Technology Services Department (CITS) is responsible for the management and allocation of bandwidth in this medium. This process is administered through the use of Wireless Access Points (WAPs). WAPs refer to devices which serve as a connection between wireless and wired technologies. This includes all forms of wireless networking, such as hardware, software, and wireless telephones including Radio Frequency (RF) and Infra-Red (IR) devices. The following processes apply to the use of the College's airwaves for voice and data transport:

- All wireless access points must be pre-approved and registered by CITS prior to being deployed for service;
- All wireless access points must be secured from unauthorized use. Appropriate forms of authentication and authorization will vary depending on the wireless medium.

2.6 Patch Controls

Reasonable attempts must be made to secure servers against published security vulnerabilities. This includes the timely application of patches, service packs, and hot fixes to operating systems and applications, as long as the corrective action itself will not adversely affect the proper operation of the server. The following controls apply to networked computers and servers:

- Critical operating system patches must be installed on all systems;
- Critical application patches must be installed on all systems.

2.7 Anti-Virus Controls

All networked computers and servers must have anti-virus protection installed. The following controls apply:

- An anti-virus software must be installed on all systems;
- The most recent version of anti-virus software must be maintained with current virus signature/patterns on all systems.

2.8 Backup and Recovery Controls

In an effort to preserve the College's information in the event of a partial or total loss of information technology resources, the Computer Information Technology Services (CITS) Department applies the following controls to servers:

- The servers and the HP mainframe containing "critical" data is managed by CITS and routinely backed up;
- Network devices necessary to the continued operation of the College's network services are maintained on a hardware support plan. This provides recovery from any hardware failure within 4 to 72 hours;
- Network devices critical to the continued operation of the College's network services are configured in fault-tolerant designs or utilizing on-site spares where ever possible;
- Data that has been backed up is tested periodically to ensure that the media and restoration procedures are functioning and that the data is actually retrievable;
- Full backups are stored at both onsite and offsite locations.

2.9 Software Controls

In accordance with the terms of software applications and compliance with copyright laws, the College exercises the following controls regarding the installation and use of software on all computing devices owned or leased by Baltimore City Community College (BCCC):

- All software that is installed on computing devices must be licensed through the College
- Software installations must be performed by a CITS technician
- Licensing information for standard software applications must be maintained by CITS
- CITS will perform licensing audits on standard software applications

In addition to the above-mentioned software controls, the College enforces same through policies development (referenced in the *CITS Policies and Procedures Manual* and *the BCCC Center*), including but not limited to:

- Software Use for Faculty and Staff;
- Faculty and Staff Computer Use & Internet Access;
- Student Computer Use & Internet Access;
- Faculty and Staff Wireless Use;
- Student Wireless Use.

SECTION 3: IT Incident Response Policy

Baltimore City Community College follows a systematic process for identifying, tracking, and responding to information security incidents. The coordination of all activities related to an IT Incident Response will aid in protecting the confidentiality, integrity, and availability of the College's information and information technology resources, as well as accelerate the remediation cycle. The College reserves the right to take necessary action under this policy to protect its resources and/or preserve evidence.

3.0 IT Incident Response Process

In the event of an information security incident or breach, the College will undertake the necessary processes to remedy the incident or breach, in hopes of preserving the College's information and information technology resources.

3.1 Information Technology Response Team

Information Technology Response Team (ITRT). A team of IT professionals assembled to address a breach or information security event or incident. The team consists of the:

- Director of Campus Resource;
- Network Administrators;
- IT Infrastructure/Security Officer;
- Systems Analysts;
- Data Security Officer;
- IT Quality Assurance Manager;
- Chief Information Technology Officer (for reporting purposes).

3.2 Classification

In this plan, an information security incident falls into one of two categories: A high severity incident and a low severity incident. The Chief Information Technology Officer (CITO) or designee is responsible for escalating a reported event to an incident, and initiating an incident response, according to the classification described below.

A **high severity incident** involves unauthorized access to information, loss or theft of a device known to store, process, or transmit highly sensitive information. Also, a high severity incident includes, but is not limited to, a compromised networking device such as a router or switch; an unauthorized change in the configuration of a firewall, an intrusion detection system, or a Tripwire; the unavailability of a critical system needed to perform daily transactions; a wide-spread attack on critical and non-critical College's systems; infrastructure failure; and any of the hazards mentioned in *Baltimore City Community College's Emergency Operations Plan* that pose a threat to operations of the College.

A **low severity incident** involves any information security incident that does not fall in the high severity classification.

3.3 Initial Report and Assessment

The processes relevant to reporting and assessment specify actions required by Baltimore City Community College's (BCCC) personnel reporting or responding to an information security event or incident that may threaten the confidentiality, integrity, and availability of the College's information and information technology resources. These processes include but are not limited to:

- All members of the College are responsible for reporting known or suspected information security events promptly to the Service Desk or the Computer Information Technology Services (CITS) Department via email or telephone:-
    - Service Desk - helpdesk@bccc.edu or 410-462-7420
    - CITS Department – 410-462-8563
- The Service Desk staff person receiving the report will contact the appropriate personnel for the system. If the reported event appears to meet one or more high severity criteria described in Section 3.2 of this plan, the Service Desk staff person will contact the CITO or designee to evaluate the event;
- The CITO or designee is responsible for escalating a reported event to an incident, and initiating an incident response. All incidents will follow the processes defined in this document. However, if the CITO or designee declares the reported event, as an incident that requires an emergency response, then the response must follow the procedures identified in *Baltimore City Community College's Emergency Operations Plan;*
- All individuals involved in reporting or investigating an information security event or incident are obliged to maintain confidentiality, unless the CITO or designee authorizes information disclosure;
- Any exceptions to these processes must be approved by the CITO or designee.

3.4 Mitigation and Containment

Upon notification of a potential breach, a system administrator shall take the necessary actions to immediately terminate unauthorized access by an intruder, eliminate the method of access used by the intruder, and eradicate any related vulnerabilities. Systems that have been infected with malicious code or systems accessed by an intruder shall be isolated from the network, until the extent of the damage can be assessed.

3.5 Response and Investigation

All declared information security incidents will warrant a priority response from the Information Technology Response Team (ITRT). The response will encompass protecting the College's information and information technology resources, containing any damage or spread, preserving evidence, eradicating damage, and restoring systems. Also, during the response and investigation

phases, the CITO or designee will be responsible for communicating with other College personnel or officials for the purpose of update and instruction, for the duration of the incident.

During the investigation of the incident, every effort shall be made to preserver log and system files that could be used as evidence of an information security incident. This may include backing up the affected system(s), documenting all activities performed on the affected system(s), storing drives and tapes in secured safes, and documenting and controlling the movement and handling of potential evidence in an effort to maintain a sense of guardianship. The ITRT shall serve as the central point for collection of evidence.

In conjunction with the investigation of an incident, the college will follow the business continuity plan defined in the College's disaster recovery plan so that critical business activities will not come to a halt, or if so, only for a minimum amount of time. However, business continuity will not take precedence over the activities necessary to contain damage or preserve evidence. Therefore, individual departments must be prepared to handle an interruption in service as a result of actions needed to contain and remedy the incident. Thus, all departments within the College are required to have a business continuity plan in place so that critical College business will not be discontinued during an unforeseen circumstance, including but not limited to, an information security incident or any of the hazards mentioned in *Baltimore City Community College's Emergency Operations Plan.*

3.6 Eradication and Restoration

The Information Technology Response Team (ITRT) will determine the extent of damage to the system(s) affected by the incident. If the damage is severe and the integrity of the information data is controversial, this may required that the system(s) be shutdown and a complete restoration of the operating systems and data be initiated. The CITO or designee must notify the appropriate College officials if in fact a critical system must be taken off-line for an extended period of time in order to perform a system restoration.

3.7 Documentation and Final Report

Disseminating information to the appropriated personnel is an essential process in the response to an incident. If an incident extends beyond 4 hours, the individual directly involved in addressing the incident should provide the CITO and their immediate supervisor with updates on the status of the incident and the remediation efforts.

The Information Technology Response Team is responsible for preparing documentation for the incident report. The actual report should be submitted by an individual directly involved in addressing the incident. All information relevant to the incident must be written on the ***IT Incident Report Form*** and filed within three business days of the conclusion of the incident. The incident report should include the following information:

- The name of individual submitting the report;

- The affected system(s) and their respective location(s);
- A description of the system(s) including hardware, operating system, application software, and the function or purpose of the system;
- A description of the information security incident;
- An assessment of the damage or loss;
- The status of the system in terms of incident resolution;
- The corrective action(s) taken to resolve damage or loss to the system(s).

The Chief Information Technology Office (CITO) shall manage the dissemination of incident information to College officials, including but not limited to the President, Vice Presidents, and the Director of Public Safety. Additionally, the College will comply with any reporting requirements imposed by state and federal laws, including but not limited to, the State of Maryland, Department of Information Technology, the Attorney General's Office (AGO), and law enforcement if the incident could affect the public or imposes user misconduct or criminal activities. The dissemination of incident information either from the CITO or through the College shall be handled appropriately in order to reduce exposure of sensitive information.

3.8 Incident Prevention

The continuous development of processes for the configuration of the College's information and information technology resources is critical to the ongoing initiative of protecting the confidentiality, integrity, and availability of information. Therefore, Baltimore City Community College will monitor, scan, and test its information technology infrastructure annually for anomalies to prevent information security incidents.

SECTION 4: Disaster Recovery Plan

Baltimore City Community College's (BCCC) IT systems are vital resources needed to conduct business processes. Notably, the College's success is dependent upon the services that these IT systems provide; thus, is crucial that these systems be operational without unnecessary interruption. To that end, the College has established an IT Disaster Recovery Plan outlining the procedures that facilitate an effective and expedient system recovery, subsequent to a service disruption or disaster. BCCC's IT Disaster Recovery Plan is a comprehensive document that is separate from this document.

SECTION 5: Security Awareness

Baltimore City Community College ensures that users understand their roles and responsibilities for information security through ongoing awareness. The focus on IT security concerns and how users should respond to those concerns are paramount to minimizing security events or incidents. Therefore, the College promotes awareness through existing policies, procedures, and standard operating procedures. Also, the Computer Information Technology Services (CITS) Department presents awareness materials through email notifications such as CITS Alerts, CITS Tips, and CITS Updates. Additionally, CITS provides documentation to individuals accessing "critical"

information, such as the Password Release Form, etc. CITS works in conjunction with the Human Resources Department to provide IT system information to new users during orientation.

The College is committed to enhancing programs and services for all stakeholders. With that said, the security awareness initiatives will be evaluated and revised on an annual basis. Thus, there will be opportunities to implement more mechanisms to address security awareness effectively in the BCCC community.

SUMMARY

Baltimore City Community College's Information Technology Security Plan identified the security requirements deemed necessary by the State of Maryland, Department of Information Technology (DOIT) to protect the confidentiality, integrity, and availability of information and information technology resources. In addition to the state, the plan is in compliance with federal laws pertaining to safeguards and privacy of information. The plan focuses on five (5) essential areas of security: IT Security Policy, Risk Management Process, IT Incident Response Process, Disaster Recovery Plan, and Security Awareness.

This Information Technology Security Plan is enforced and supported by BCCC's policies, procedures, standard operating procedures, and state and federal laws. Specifically, the plan identifies the necessary safeguards and processes to protect the College's information from unauthorized access, modification, disclosure, and destruction. All stakeholders, including but not limited to faculty, staff, students, alumni, board members, members of the community, vendors, contractors, affiliations, and partners are required to comply with these processes and controls documented in this plan, as well as, all other College policies and procedures. This plan shall be reviewed and updated once every two years.