W. L. BONNER COLLEGE
INFORMATION SECURITY POLICIES

Preliminary Edition

July 1, 2012

Office of Technology Services
W. L. Bonner College
Columbia, SC 29203-5901

W. L. BONNER COLLEGE INFORMATION SECURITY POLICIES

INTRODUCTION

The *W. L. Bonner Information Security Policies: Preliminary Edition* has been created to help protect the College from security threats that could compromise the College's right to privacy, productivity, reputation, and electronic information. This policy document recognizes the vital role information plays in the College's educational, administrative and community service functions. The information contained within this document must be protected at all cost as more information is used and shared by students, faculty, and staff. These policies serve to protect information resources from threats both within and outside of the College by setting forth guidelines, responsibilities, and practices that will help the College prevent, detect, and respond to situations that compromise the College's integrity.

The Dean-CEO of the W. L. Bonner College delegates to the Manager, Technology Services, in the Office of Technology Services the responsibility for compliance with these policies.

TABLE OF CONTENTS

W. L. Bonner College

SECTION:	**INFORMATION SECURITY POLICIES – GENERAL**	**EFFECTIVE DATE: 7/1/2012**
SUBJECT:	**INFORMATION SECURITY POLICY**	**REVISED:**
POLICY #:	**TS-1**	**REVIEWED:**

TS-1 INFORMATION SECURITY POLICY:

It is the policy of W. L. Bonner College to protect the College and its interests from information security threats that could compromise the College's right to privacy, productivity, reputation, and electronic information. This statement recognizes the complexity of the challenges facing the College in this regard, and in particular, addresses both general and individual policies affecting administrative and technical responsibilities associated with Network Access, Academic Lab Security, Data Level Security, Application Service Providers (ASP) Security Standards, Network Device Policies, Acceptable Use Policy, and Risk/Audit Policies. This WLBC Information Security Policy is issued in direct compliance with the guidelines and directives of the Association of Biblical Higher Education (ABHE), the accrediting body for WLBC.

ADMINISTRATION:

The Dean-CEO of the W. L. Bonner College delegates to the Manager, Technology Services, in the Office of Technology Services the responsibility for compliance with these policies.

IMPLEMENTATION:

1. The Manager, Technology Services, in the Office of Technology Services has the responsibility for establishing and coordinating all information security requirements relating to computer and/or network generated information, and the processing of the data with EDP equipment.
2. Information Security Safeguards
   Measures relating to the processing of data will be taken to ensure against the unauthorized access, modification, destruction, and disclosure of information whether accidental or intentional. Information Security Safeguards will be established to ensure integrity and accuracy of vital W. L. Bonner College data.
3. Scope
   The policy applies strictly to computerized activities and information only while in the custodial care of the data processing function.

4. Responsibilities

   The data processing security function within the Office of Technology Services shall be responsible for implementing this policy under the oversight and authority of the Manager, Technology Services.

   Information Security will establish such standards, procedures and guidelines as may be necessary to ensure data and physical security procedures in all areas within the jurisdiction of the data processing functions.

   It is the responsibility of each Office of Technology Services employee to adhere to these security procedures, to report to Office of Technology Services management any known violations, and to recommend additional procedures where needed.

GENERAL POLICIES:

1. Data processing facilities are to be used for W. L. Bonner College business only. The use of these facilities for personal use is strictly forbidden.
2. All information obtained through the use of data processing facilities must be maintained with the strictest confidence, and must be utilized only for purposes required by official job responsibilities.
3. Personal passwords and other means of access to specific information systems facilities must not be divulged to anyone.
4. Employees are responsible for any use of equipment or access to data under their user ID. Leaving a computer signed on leaves the employee responsible for its use.
5. Computers, terminals, and related communication and other peripheral computer equipment to include printed reports, shall be protected against physical abuse or unauthorized use.
6. All systems will be configured to terminate the session of any terminal connected to it after a period of 20 minutes of inactivity.
7. Copies of any programs or data may not be permanently removed from any system data sets unless required management approval is obtained.
8. Personal computer users are responsible for insuring adequate physical security for their equipment and their data. Access to data on diskettes or personal computers disk should be controlled. Measures should be taken to assure that backup copies of critical data are made, and where necessary, stored offsite.
9. Copyrighted or patented software purchased or developed by Academic Information Services (AIS) personnel is the property of W. L. Bonner College and must not be duplicated without the permission of the owner.
10. Violations of these policies could result in termination of employment.

W. L. Bonner College

SECTION: NETWORK ACCESS POLICIES EFFECTIVE DATE: 7/1/2012
POLICIES

SUBJECT: NETWORK ACCESS SECURITY POLICY REVISED:

POLICY #: NA-1 REVIEWED:

NA -1NETWORK ACCESS SECURITY POLICIES:

Authorized W. L. Bonner College Information Services are provided to all faculty members, staff, students and other authorized individuals through the resources of the Bonner College Network (BCN). The BCN hosts a variety of information stores the availability and validated accessibility of which can be securely ensured, and its validity, integrity, and currency religiously maintained, consistent with the mission and vision of the College, and to the benefit of all of its constituents both inside and outside of the College. In particular, Network Access Security Policies rely heavily upon the strength, structure and durability of authorized Passwords. Passwords are an critically important aspect of Network Access Security. They are the front line of protection for access to network-based user accounts. Thus, the BCN and a secured password system are vital and essential components of the technology infrastructure the access to and use of which must be perpetually secured, protected and insured in direct compliance with the guidelines and directives of the Association of Biblical Higher Education (ABHE), the accrediting body for WLBC.

ADMINISTRATION:

The Dean-CEO of the W. L. Bonner College delegates to the Manager, Technology Services, in the Office of Technology Services the responsibility for compliance with these policies.

IMPLEMENTATION:

NETWORK ACCESS PASSWORD POLICY:

1. Overview
The importance of appropriate Network Access Passwords cannot be overstated as an important aspect of information security. They are the front line of protection for user accounts. A poorly constructed password may result in the compromise of W. L. Bonner College's entire Enterprise network. As such, all W. L. Bonner College faculty members, students, staff members and other employees (including contractors and vendors with access to W. L. Bonner College systems) are responsible for taking the appropriate steps, as outlined below, to select, secure and utilize their passwords appropriately.

2. Purpose
The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3. Scope
The scope of this policy includes all personnel (faculty, staff, students, and contractors) who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any W. L. Bonner College Network facility (BCN), has access to the W. L. Bonner College network, or stores any non-public W. L. Bonner College information.

4. Policy - General

4.1 All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed every ninety days. The recommended change interval is every three months.
4.2 Passwords must not be inserted into email messages or other forms of electronic communication.
4.3 All user-level and system-level passwords must conform to the guidelines described below.

5. General Password Construction Guidelines
Passwords are used for various purposes at W.L Bonner College. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select and/or construct strong passwords.

5.1 Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - The words "WLBC College ", "sanjose", "sanfran" or any derivation.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

5.2 Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)

- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Passwords are at least eight alphanumeric characters long
- Passwords are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use any of these examples as passwords!

6. Password Protection Standards
   Do not use the same password for W. L. Bonner College accounts as for other non -W. L. Bonner access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various W, L. Bonner College access needs. For example, select one password for the ABHE systems and a separate password for PBWORKS systems. Also, select a separate password to be used for an NT account and a UNIX account.

   Do not share W. L. Bonner College passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential W. L. Bonner College information.

   Here is a list of "don’ts":

   - Don't reveal a password over the phone to ANYONE
   - Don't reveal a password in an email message
   - Don't reveal a password to the boss
   - Don't talk about a password in front of others
   - Don't hint at the format of a password (e.g., "my family name")
   - Don't reveal a password on questionnaires or security forms
   - Don't share a password with family members
   - Don't reveal a password to co-workers while on vacation

   If someone demands a password, refer them to this document or have them call someone in the Office of Technology Services.

   Do not use the "Remember Password" feature of applications (e.g., Eudora, OutLook, Netscape Messenger).

   Again, employees are directed not to write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including smart phones, tablets or other mobile devices) without encryption.

Change passwords at least once every 60 days (except system-level passwords which must be changed quarterly). The recommended change interval is every four months.

If an account or password is suspected to have been compromised report the incident to OTS and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by OTS or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

7. Application Development Standards

Application developers must ensure their programs contain the following security precautions. Applications:

- Should support authentication of individual users, not groups.
- Should not store passwords in clear text or in any easily reversible form.
- Should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

8. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

W. L. Bonner College

SECTION:	ACADEMIC LABORATORY SECURITY POLICIES	EFFECTIVE DATE: 7/1/2012
SUBJECT:	ACADEMIC LABORATORY SECURITY POLICY	REVISED:
POLICY #:	AL-1	REVIEWED:

AL-1 ACADEMIC LABORATORY SECURITY POLICY:

1. Purpose

This policy establishes information security requirements for all networks and equipment deployed in W. L. Bonner College Academic Laboratories which are hosted by the Bonner College Network (BCN). Adherence to these requirements will minimize the potential risk to the W. L. Bonner College from damage cause by unauthorized use of W. L. Bonner College resources, and the loss of sensitive confidential data and intellectual property.

2. Scope

All W. L. Bonner College Computer Laboratories hosted by the Bonner College Network (BCN) and devices (including but not limited to routers, switches, hosts, etc.) that are Internet facing are considered part of the Academic Laboratories and are subject to this policy. This includes the present Academic Laboratory and any future such laboratory in primary Internet Service Provider (ISP) locations as well as remote locations. All existing and future equipment, which falls under the scope of this policy, must be configured according to the referenced documents.

3. Policy

3.1 Ownership and Responsibilities

3.1.1 All new Academic Laboratories must present a business justification with sign-off at the Dean’s level. The Information Systems Security Administration (OTS) function within the Office of Technology Services must keep the business justifications on file.

3.1.2 Laboratory owning organizations within the College are responsible for assigning Laboratory Managers; point of contact (POC) personnel, and back up POC personnel, for each laboratory. The laboratory owners must maintain up to date POC information with the Office of Technology Services Information Security Services Administration (ISSA) function. Laboratory managers or assigned POC personnel must be available throughout the hours of operation of the laboratory, and especially for emergencies.

3.1.3 Changes to the network connectivity and/or purpose of existing Academic Laboratories and/or the establishment of new Academic Laboratories must be coordinated with the Office of Technology Services and approved by the ISSA function within that office.

3.1.4 All ISP connections must be maintained and approved by the Office of Technology Services.

3.1.5 Office of Technology Services Network Services staff must maintain a firewall device between any and all Academic Laboratories and the Internet.

3.1.6 All Academic Laboratories will provide and maintain network devices deployed in the Academic Laboratory up to point of demarcation identified by the Bonner College Network (BCN) as managed by Office of Technology Services.

3.1.7 The Network Services staff and the ISSA function within the Office of Technology Services reserve the right to interrupt laboratory connections if a security concern exists.

3.1.8 The Network Services staff and the ISSA function within the Office of Technology Services must record all Academic Laboratory address spaces and current contact information.

3.1.9 The Lab Managers are ultimately responsible for their Academic Labs complying with this policy.

3.1.10 Immediate access to equipment and system logs must be granted to the OTS and Network Services staff within the Office of Technology Services upon request, and comply with W. L. Bonner College *Audit Policy*

3.1.11 The ISSA function within the Office of Technology Services will address non-compliance waiver requests on a case-by-case basis.

3.2 General Configuration Requirements

3.2.1 Production resources must not depend upon resources on the Academic Laboratory networks.

3.2.2 Academic Laboratories should be in a physically separate room from any internal networks. If this is not possible, the equipment must be in a locked rack with limited access. In addition, the Laboratory Manager must maintain a list of who has access to the equipment.

3.2.3 Laboratory managers are responsible for complying with the following related policies:

Password Policy
Wireless Communications Policy
Academic Laboratory Anti-Virus Policy

3.2.4 Firewall devices maintained by Office of Technology Services Network Services staff must be configured in accordance with least-access principles and the Laboratory business needs. All firewall filters will be maintained by the Office of Technology Services' Network Services staff.

3.2.5 The firewall device must be the only access point between the Laboratory and the rest of Bonner College Network (BCN) and/or the Internet. Any form of cross-connection, which bypasses the firewall device, is strictly prohibited.

3.2.6 Original firewall configurations and any changes thereto must be reviewed and approved by the ISSA function (including both general configurations and rule sets). The ISSA function may require additional security measures as needed.

3.2.7 Traffic from Academic Laboratories to the Bonner College Network (BCN) including VPN access, falls under the *Remote Access Policy.*

3.2.8 All routers and switches not used for testing and/or training must conform to the BCN Router and Switch standardization documents.

3.2.9 Operating systems of all hosts internal to the Academic Laboratory running Internet Services must be configured to the secure host installation and configuration standards.

3.2.10 Current applicable security patches/hot-fixes for any applications that are Internet services must be applied. Administrative owner groups must have processes in place too stay current on appropriate patches/hotfixes.

3.2.11 All applicable security patches/hot-fixes recommended by the vendor must be installed. Administrative owner groups must have processes in place to stay current on appropriate patches/hotfixes.

3.2.12 Services and applications not serving business requirements must be disabled.

3.2.13 W. L. Bonner College Confidential Information is prohibited on equipment in labs where non- W. L. Bonner College personnel have physical access (e.g., training labs), in accordance with the *Information Sensitivity Policy*.

3.2.14 Remote administration must be performed over secure channels (e.g., encrypted network connections using SSH or IPSEC) or console access independent from the Academic Laboratory internal networks.

4. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action up to and including termination of employment.

5. Definitions

Terms Definitions

Access Control List (ACL) Lists kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).

Academic Labs Networking that exists outside of W. L. Bonner College primary Enterprise firewalls but is still under W. L. Bonner College administrative control.

Network Support Organization Any OTS-approved support organization that manages the networking of non-lab networks.

Least Access Principle Access to services, hosts, and networks is restricted unless otherwise permitted.

Internet Services Services running on devices that are reachable from other devices across a network. Major Internet services include DNS, FTP, HTTP, VPN etc.

Network Support Organization Point of Demarcation The point at which the networking responsibility transfers from a Network Support Organization to the Academic Laboratory. Usually a router or firewall.

Laboratory Manager

The individual responsible for all laboratory activities and personnel.

Laboratory

A Laboratory is any non-production environment, intended specifically for developing, demonstrating, training and/or student use.

Firewall

A device that controls access between networks. such as a PIX, a router with access control lists, or a similar security device approved by OTS.

Internally Connected Lab

A laboratory within W. L. Bonner College's Enterprise firewall and connected to the BCN.

W. L. Bonner College

SECTION: GENERAL PC SECURITY POLICY EFFECTIVE DATE: 7/1/2012

SUBJECT: ANTI-VIRUS POLICY REVISED:

POLICY #: PC-1 REVIEWED:

TS-4 ANTI-VIRUS POLICY:

1. Purpose

This policy establishes requirements that must be met by all computers and information-based devices connected to the Bonner College Network (BCN) to ensure effective virus detection and prevention.

2. Scope

This policy applies to all W. L. Bonner laboratory or academic and administrative computers that are PC-based or utilize PC-file directory sharing, and that access information resources via the Bonner College Network (BCN). This includes, but is not limited to desktop computers, laptop computers, file/ftp/tftp/proxy servers, and any PC based lab equipment such as traffic generators.

3. Policy

All W. L. Bonner College PC-based computers must have W. L. Bonner College's standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. The Office of Technology Services is responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into W. L. Bonner College Network (BCN), e.g., viruses, worms, Trojan horses, e-mail bombs, etc., are prohibited, in accordance with the *Acceptable Use Policy*.

4. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

W. L. Bonner College

SECTION:	**DATA LEVEL POLICIES**	**EFFECTIVE DATE: 7/1/2012**
SUBJECT:	**ACCEPTABLE ENCRYPTION POLICY**	**REVISED:**
POLICY #:	**DL-1**	**REVIEWED:**

DL-1 ACCEPTABLE ENCRYPTION POLICY:

1. Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

2. Scope

This policy applies to all W. L. Bonner College employees and affiliates.

3. Policy

Proven, standard algorithms such as DES, RSA, RC5 and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Network Associate's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or Diffie-Hillman, while Secure Socket Layer (SSL) uses RSA encryption. Symmetric cryptosystem key lengths must be at least 56 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. The key length requirements of identified vendors will be reviewed annually and upgraded as technology allows.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the OTS. Be aware that the U.S. Government restricts the export of encryption technologies. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

4. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Definitions

Term	**Definition**
Proprietary Encryption	An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.

Symmetric Cryptosystem A method of encryption in which the same key is used for both encryption and decryption of the data.

Asymmetric Cryptosystem A method of encryption in which two different keys is used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

DES Data Encryption Standard a popular symmetric encryption method.

RSA A public –key encryption technology developed by RSA Data Security.

W. L. Bonner College

SECTION: DATA LEVEL POLICIES EFFECTIVE DATE: 7/1/2012

SUBJECT: GUIDELINES ON ANTI-VIRUS PROCESS REVISED:

POLICY #: DL-2 REVIEWED:

TS-6 GUIDELINES ON ANTI-VIRUS PROCESS:

1. Recommended Processes to Prevent Virus Problems:
   - 1.1 Always run the W. L. Bonner College standard, supported anti-virus software available from the Office of Technology Services download site. Download and run the current version; download and install anti-virus software updates as they become available.
   - 1.2 NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
   - 1.3 Delete spam, chain, and other junk email without forwarding, in accordance with W. L. Bonner College 's *Acceptable Use Policy*.
   - 1.4 Never download files from unknown or suspicious sources.
   - 1.5 Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
   - 1.6 Always scan a thumb drive, CD or DVD from an unknown source for viruses before using it.
   - 1.7 Back-up critical data and system configurations on a regular basis and store the data file in a safe place.
   - 1.8 If laboratory testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, then run the laboratory test. After the laboratory test, enable the anti-virus software. When the anti-virus softwareis disabled, do not run any applications that could transfer a virus, e.g., email or file sharing apps.
   - 1.9 New viruses are discovered almost every day. Periodically check the *Anti-Virus Policy* and this Recommended Processes list for updates.

W. L. Bonner College

SECTION: DATA LEVEL POLICIES **EFFECTIVE DATE: 7/1/2012**

SUBJECT: AUTOMATICALLY FORWARDED EMAIL POLICY **REVISED:**

POLICY #: DL-3 **REVIEWED:**

DL-3 AUTOMATICALLY FORWARDED EMAIL POLICY:

1. Purpose

The purpose of this policy is to prevent the unauthorized or inadvertent disclosure of sensitive W. L. Bonner College information.

2. Scope

This policy covers automatic email forwarding, and thereby the potentially inadvertent transmission of sensitive information by all employees, vendors, and agents operating on behalf of the W. L. Bonner College.

3. Policy

Employees must exercise utmost caution when sending any email from inside the W. L. Bonner College to an outside network. Unless approved by an employee's manager or the ISSA function in the Office of Technology Services, W. L. Bonner College email will not be automatically forwarded to an external destination. Sensitive information, as defined in the *Information Sensitivity Policy*, will not be forwarded via any means, unless that email is critical to business and is encrypted in accordance with the *Acceptable Encryption Policy*.

4. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Definitions

Term	Definition
Email	The electronic transmission of information through a mail protocol such as SMTP. Programs such as Eudora and Microsoft Outlook use SMTP.
Forwarded email	Email resent from internal networking to an outside point.
Sensitive information	Information is considered sensitive if it can be damaging to the W. L. Bonner College or its employees, students or reputation.
Unauthorized Disclosure	The intentional or unintentional revealing of restricted information to people who do not have a need to know that information.

W. L. Bonner College

SECTION:	**APPLICATION SERVICE PROVIDER (ASP) SECURITY STANDARDS**	**EFFECTIVE DATE: 7/1/2012**
SUBJECT:	**APPLICATION SERVICE PROVIDER (ASP) SECURITY STANDARDS**	**REVISED:**
POLICY #:	**ASP-1**	**REVIEWED:**

ASP-1 APPLICATION SERVICE PROVIDER (ASP) SECURITY STANDARDS:

1. Purpose

The purpose of this policy is to define the minimum-security criteria that an Application Service Provider (ASP) must meet in order to be considered for use by W. L. Bonner College. As part of the ASP selection process, the ASP Vendor must demonstrate compliance with the Standards listed below by responding in writing to EVERY statement and question in the six categories. OTS will closely review the vendor responses, and will suggest remediation measures in any areas that fall short of the minimum-security criteria. Approval of any given ASP by the Information Security (OTS) function in the Office of Technology Services resides largely on the vendor's response to this document.

These Standards are subject to additions and changes without warning by OTS.

2. Scope

This document can be provided to ASPs that are either being considered for use by the W. L. Bonner College, or have already been selected for use.

3. Responding To These Standards

OTS is looking for explicitly detailed, technical responses to the following statements and questions. ASPs should format their responses directly beneath the Standards (both questions and requirements) listed below. In addition, please include any security white papers, technical documents, or policies that you may have.

Answers to each Guideline should be specific and avoid generalities, e.g.:

Examples:

Bad: "We have hardened our hosts against attack."
Good: "We have applied all security patches for Windows 2010 as of 4/31/2012 to our servers. Our Administrator is tasked with keeping up-to-date on current vulnerabilities that may affect our environment, and our policy is to apply new patches during our maintenance period (2300hrs, Saturday) every week. Critical updates are implemented within 24 hours. A complete list of applied patches is available to W. L. Bonner College."

Bad: "We use encryption."
Good: "All communications between our site and W. L. Bonner College will be protected by IPSec ESP Tunnel mode using 168-bit TripleDES encryption, SHA-1 authentication. We exchange authentication material via either out-of-band shared secret, or PKI certificates."

4. Standards

4.1 General Security

1. W. L. Bonner College reserves the right to periodically audit the W. L. Bonner College application infrastructure to ensure compliance with the ASP Policy and these Standards. Non-intrusive network audits (e.g., basic port scans, etc.) may be done randomly, without prior notice. More intrusive network and physical audits may be conducted on site with 24 hours notice.
2. The ASP must provide a proposed architecture document that includes a full network diagram of the W. L. Bonner College Application Environment, illustrating the relationship between the Environment and any other relevant networks, with a full data flowchart those details where W. L. Bonner College data resides, the applications that manipulate it, and the security thereof.
3. The ASP must be able to immediately disable all or part of the functionality of the application should a security issue be identified.

4.2 Physical Security

1. The equipment hosting the application for W. L. Bonner College must be located in a physically secure facility, which requires badge access at a minimum.

2. The infrastructure (hosts, network equipment, etc.) hosting the W. L. Bonner College application must be located in a locked cage-type environment.

3. W. L. Bonner College shall have final say on who is authorized to enter any locked physical environment, as well as access the W. L. Bonner College Application Infrastructure.

4. The ASP must disclose who amongst their personnel will have access to the environment hosting the application for W. L. Bonner College.

5. W. L. Bonner College's Enterprise Asset Protection team requires that the ASP disclose their ASP background check procedures and results prior to OTS granting approval for use of an ASP.

4.3 Network Security

1. The network hosting the application must be air-gapped from any other network or customer that the ASP may have. This means the W. L. Bonner College application environment must use separate hosts, and separate infrastructure.

2. How will data go between W. L. Bonner College and the ASP? Keep in mind the following two things:

a. If W. L. Bonner College will be connecting to the ASP via a private circuit (such as frame relay, etc.), then that circuit must terminate on the W. L. Bonner College extranet, and the operation of that circuit will come under the procedures and policies that govern the W. L. Bonner College Partner Network Management Group.

b. If, on the other hand, the data between W. L. Bonner College and the ASP will go over a public network such as the Internet, the ASP must deploy appropriate fire walling technology, and the traffic between W. L. Bonner College and the ASP must be protected and authenticated by cryptographic technology (See Cryptography below).

4.4 Host Security

1. The ASP must disclose how and to what extent the hosts (Unix, NT, etc.) comprising the W. L. Bonner College application infrastructure have been hardened against attack. If the ASP has hardening documentation for the CAI, provide that as well.

2. The ASP must provide a listing of current patches on hosts, including host OS patches, web servers, databases, and any other material application.

3. Information on how and when security patches will be applied must be provided. How does the ASP keep up on security vulnerabilities, and what is the policy for applying security patches?

4. The ASP must disclose their processes for monitoring the integrity and availability of those hosts.

5. The ASP must provide information on their password policy for the W. L. Bonner College application infrastructure, including minimum password length, password generation guidelines, and how often passwords are changed.

6. W. L. Bonner College cannot provide internal usernames/passwords for account generation, as the ASP is not comfortable with internal passwords being in the hands of third parties. With that restriction, how will the ASP authenticate users? (e.g., LDAP, Netegrity, Client certificates.)

7. The ASP must provide information on the account generation, maintenance and termination process, for both maintenance as well as user accounts. Include information as to how an account is created, how account information is transmitted back to the user, and how accounts are terminated when no longer needed.

4.5 Web Security

1. At W. L. Bonner College 's discretion, the ASP may be required to disclose the specific configuration files for any web servers and associated support functions (such as search engines or databases).

2. Please disclose whether, and where, the application uses Java, Javascript, ActiveX, PHP(Hypertext Preprocessor) or ASP (active server page) technology.

3. What language is the application back-end written in? (C, Perl, Python, VBScript, etc.)

4. Please describe the ASP process for doing security Quality Assurance testing for the application. For example, testing of authentication, authorization, and accounting functions, as well as any other activity designed to validate the security architecture.

5. Has the ASP done web code review, including CGI, Java, etc, for the explicit purposes of finding and remediating security vulnerabilities? If so, who did the review, what were the results, and what remediation activity has taken place? If not, when is such an activity planned?

4.6 Cryptography

1. The W. L. Bonner College application infrastructure cannot utilize any "homegrown" cryptography – any symmetric, asymmetric or hashing algorithm utilized by the W. L. Bonner College application infrastructure must utilize algorithms that have been published and evaluated by the general cryptographic community.

2. Encryption algorithms must be of sufficient strength to equate to 168-bit Triple DES.

3. Preferred hashing functions are SHA-1 and MD-5.

4. Connections to the ASP utilizing the Internet must be protected using any of the following cryptographic technologies: IPSec, SSL(Secure Sockets Layer), SSH(Secure Shell), PGP(Pretty Good Privacy).

5. If the W. L. Bonner College application infrastructure requires PKI, please contact W. L. Bonner College Information Security Group for additional guidance.

W. L. Bonner College

SECTION: NETWORK DEVICE POLICIES **EFFECTIVE DATE: 7/1/2012**

SUBJECT: ROUTER SECURITY POLICY **REVISED:**

POLICY #: ND-1 **REVIEWED:**

ND-1 ROUTER SECURITY POLICY:

1. Purpose

This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of W. L. Bonner College.

2. Scope

All routers and switches connected to W. L. Bonner College production networks are affected. Routers and switches within internal, secured labs are not affected.

3. Policy

Every router must meet the following configuration standards:

1. No local user accounts are configured on the router. Routers must use TACACS+ for all user authentications.
2. The enable password on the router must be kept in a secure encrypted form. The router must have the enable password set to the current production router password from the router's support organization.
3. Disallow the following:
    a. IP directed broadcasts
    b. Incoming packets at the router sourced with invalid addresses such as RFC1918 address
    c. TCP small services
    d. UDP small services
    e. All source routing
    f. All web services running on router
4. Use Enterprise standardized SNMP(Simple Network Management Protocol) et community strings.
5. Access rules are to be added as business needs arise.
6. The router must be included in the College enterprise management system with a designated point of contact.

7. Each router must have the following statement posted in clear view:

"UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device."

4. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Definitions

Lab Network

A "lab network" is defined as any network used for the purposes of testing, demonstrations, training, etc. Any network that is stand-alone or fire neither walled off from the production network(s) and whose impairment will not cause direct loss to W. L. Bonner College nor affect the production network.

W. L. Bonner College

SECTION: NETWORK DEVICE POLICIES EFFECTIVE DATE: 7/1/2012

SUBJECT: SERVER SECURITY POLICY REVISED:

POLICY #: ND-2 REVIEWED:

ND-2 SERVER SECURITY POLICY:

1. Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by W. L. Bonner College. Effective implementation of this policy will minimize unauthorized access to W. L. Bonner College proprietary information and technology.

2. Scope

This policy applies to server equipment owned and/or operated by W. L. Bonner College, and to servers registered under any W. L. Bonner College-owned internal network domain.

3. Policy

3.1 Ownership and Responsibilities

All internal servers deployed at W. L. Bonner College must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by OTS. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by OTS.

- Servers must be registered within the enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
  - Server contact(s) and location, and a backup contact
  - Hardware and Operating System/Version
  - Main functions and applications, if applicable
- Information in the enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures.

3.2 General Configuration Guidelines

- Operating System configuration should be in accordance with approved OTS guidelines.
- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.

- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
- Always use standard security principles of least required access to perform a function.
- Do not use root when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.

3.3 Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
    - All security related logs will be kept online for a minimum of 1 week.
    - Daily incremental tape backups will be retained for at least 1 month.
    - Weekly full tape backups of logs will be retained for at least 1 month.
    - Monthly full backups will be retained for a minimum of 2 years.
- Security-related events will be reported to the OTS, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
    - Port-scan attacks
    - Evidence of unauthorized access to privileged accounts
    - Anomalous occurrences that are not related to specific applications on the host.

3.4 Compliance

- Audits will be performed on a regular basis by authorized organizations within W. L. Bonner College.
- Audits will be managed by the internal audit group or OTS, in accordance with the *Audit Policy*. OTS will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

4.Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.Definitions

Term	Definition
Server	For purposes of this policy, a Server is defined as an internal W. L. Bonner College Server. Desktop machines and Lab equipment are not relevant to the scope of this policy.

W. L. Bonner College

SECTION:	**ACCEPTABLE USE POLICY**	**EFFECTIVE DATE: 7/1/2012**
SUBJECT:	**ACCEPTABLE USE POLICY**	**REVISED:**
POLICY #:	**AU-1**	**REVIEWED:**

AU-1 ACCEPTABLE USE POLICY:

1. Overview

It is the intention of the Office of Technology Services (OTS) to publish an Acceptable Use Policy which does not impose restrictions that are contrary to W. L. Bonner College’s established culture of openness, trust and integrity. OTS is committed to protecting W. L. Bonner College's faculty, staff, students, partners and the organization itself from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of W. L. Bonner College. These systems are to be used for business purposes in serving the interests of the College, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every W. L. Bonner College employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at W. L. Bonner College. These rules are in place to protect the faculty, staff and students as well as the W. L. Bonner College. Inappropriate use exposes W. L. Bonner College to risks including virus attacks, compromise of network systems and services, and legal issues.

3. Scope

This policy applies to faculty, staff, contractors, consultants, temporaries, students and other workers at W. L. Bonner College, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by W. L. Bonner College.

4. Policy

4.1 General Use and Ownership

1. While W. L. Bonner College's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the College’s systems remains the property of W. L. Bonner College. Because of the need to protect W. L.

2. Bonner College's network, management cannot guarantee the confidentiality of information stored on any network device belonging to W. L. Bonner College.
3. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
4. OTS recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see OTS's Information Sensitivity Policy. For guidelines on encrypting email and documents, go to OTS's Awareness Initiative.
5. For security and network maintenance purposes, authorized individuals within W. L. Bonner College may monitor equipment, systems and network traffic at any time, per OTS's Audit Policy.
6. W. L. Bonner College reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by Enterprise confidentiality guidelines, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: College private, College strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, user level passwords should be changed every six months.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the host will be unattended.
4. Use encryption of information in compliance with OTS's Acceptable Encryption Use policy.
5. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the “Laptop Security Tips”.
6. Postings by employees from a W. L. Bonner College email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of W. L. Bonner College , unless posting is in the course of business duties.
7. All hosts used by the employee that are connected to the W. L. Bonner College Internet/Intranet/Extranet, whether owned by the employee or W. L. Bonner College , shall be continually executing approved virus-scanning software with a current virus database. Unless overridden by departmental or group policy.
8. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of W. L. Bonner College authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing W. L. Bonner College-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities, which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or college protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by W. L. Bonner College.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which W. L. Bonner College or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a W. L. Bonner College computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any W. L. Bonner College account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods,

10. packet spoofing, denial of service, and forged routing information for malicious purposes.
11. Port scanning or security scanning is expressly prohibited unless prior notification to OTS is made.
12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
13. Circumventing user authentication or security of any host, network or account.
14. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
15. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
16. Providing information about, or lists of, W. L. Bonner College employees to parties outside W. L. Bonner College.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within W. L. Bonner College 's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by W. L. Bonner College or connected via W. L. Bonner College 's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5.0 Enforcement

Any employee found to have violated this policy might be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Term	Definition
Spam	Unauthorized and/or unsolicited electronic mass mailings.

W. L. Bonner College

SECTION: ACCEPTABLE USE POLICY EFFECTIVE DATE: 7/1/2012

SUBJECT: INFORMATION SENSITIVITY POLICY REVISED:

POLICY #: AU-2 REVIEWED:

AU-2 INFORMATION SENSITIVITY POLICY:

1. Purpose

The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of W. L. Bonner College without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect W. L. Bonner College Confidential information (e.g., W. L. Bonner College Confidential information should not be left unattended in conference rooms).

Please Note: The impact of these guidelines on daily activity should be minimal.

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to ISSA.

2. Scope

All W. L. Bonner College information is categorized into two main classifications:

- W. L. Bonner College Public
- W. L. Bonner College Confidential

W. L. Bonner College Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to W. L. Bonner College.

W. L. Bonner College Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included are information that should be protected very closely, such as trade secrets, development programs, potential acquisition targets, and other information integral to the success of our organization. Also included in W. L. Bonner College Confidential is information that is less critical, such as telephone directories, general Enterprise information, personnel information, etc., which does not require as stringent a degree of protection.

A subset of W. L. Bonner College Confidential information is "W. L. Bonner College Third Party Confidential" information. This is confidential information belonging or pertaining to another corporation, which has been entrusted to W. L. Bonner College by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into W. L. Bonner College 's network to support our operations.

W. L. Bonner College personnel are encouraged to use common sense judgment in securing W. L. Bonner College Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager

3. Policy

The Sensitivity Guidelines below provides details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as W. L. Bonner College Confidential information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the W. L. Bonner College Confidential information in question.

a. Minimal Sensitivity: General Enterprise information; some personnel and technical information

   Marking guidelines for information in hardcopy or electronic form.

   Note: any of these markings may be used with the additional annotation of "3rd Party Confidential".

   Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "W. L. Bonner College Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "W. L. Bonner College Proprietary" or similar labels at the discretion of your individual business unit or department. Even if no marking is present, W. L. Bonner College information is presumed to be "W. L. Bonner College Confidential" unless expressly determined to be W. L. Bonner College Public information by a W. L. Bonner College employee with authority to do so.

   Access: W. L. Bonner College employees, contractors, people with a business need to know.
   Distribution within W. L. Bonner College: Standard interoffice mail approved electronic mail and electronic file transmission methods.

Distribution outside of W. L. Bonner College internal mail: U.S. mail and other public or private carriers, approved electronic mail and electronic file transmission methods.
Electronic distribution: No restrictions except that it is sent to only approved recipients.
Storage: Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.
Disposal/Destruction: Deposit outdated paper information in specially marked disposal bins on W. L. Bonner College premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

b. More Sensitive: Business, financial, technical, and most personnel information

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". As the sensitivity level of the information increases, you may, in addition or instead of marking the information "W. L. Bonner College Confidential" or "W. L. Bonner College Proprietary", wish to label the information "W. L. Bonner College Internal Use Only" or other similar labels at the discretion of your individual business unit or department to denote a more sensitive level of information. However, marking is discretionary at all times.

Access: W. L. Bonner College employees and non-employees with signed non-disclosure agreements who have a business need to know.
Distribution within W. L. Bonner College: Standard interoffice mail approved electronic mail and electronic file transmission methods.
Distribution outside of W. L. Bonner College internal mail: Sent via U.S. mail or approved private carriers.
Electronic distribution: No restrictions to approved recipients within W. L. Bonner College, but should be encrypted or sent via a private link to approved recipients outside of W. L. Bonner College premises.
Storage: Individual access controls are highly recommended for electronic information.
Disposal/Destruction: In specially marked disposal bins on W. L. Bonner College premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

c. Most Sensitive: Trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our College.

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". To indicate that W. L. Bonner College Confidential information is very sensitive, you may should label the information "W. L. Bonner College Internal: Registered and Restricted", "W. L. Bonner College Eyes Only", "W. L. Bonner College Confidential" or similar labels at the discretion of your individual business unit or department. Once again, this type of W. L. Bonner College Confidential information need not be marked, but users should be aware that this information is very sensitive and be protected as such.

Access: Only those individuals (W. L. Bonner College employees and non-employees) designated with approved access and signed non-disclosure agreements.
Distribution within W. L. Bonner College: Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.
Distribution outside of W. L. Bonner College internal mail: Delivered direct; signature required; approved private carriers.
Electronic distribution: No restrictions to approved recipients within W. L. Bonner College, but it is highly recommended that all information be strongly encrypted.
Storage: Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer.
Disposal/Destruction: Strongly Encouraged: In specially marked disposal bins on W. L. Bonner College premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

4. Enforcement

Any employee found to have violated this policy might be subject to disciplinary action, up to and including termination of employment.

5. Definitions

Terms and Definitions

Appropriate measures

To minimize risk to W. L. Bonner College from an outside business connection. W. L. Bonner College computer use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access W. L. Bonner College information, the amount of information at risk is minimized.

Configuration of W. L. Bonner College to other business connections

Connections shall be set up to allow other businesses to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary.

Delivered Direct; Signature Required

Do not leave in interoffice mail slot, call the mailroom for special pick-up of mail.

Approved Electronic File Transmission Methods

Includes supported FTP clients and Web browsers.

Envelops Stamped Confidential

You are not required to use a special envelope. Put your document(s) into an interoffice envelope, seal it, address it, and stamp it confidential.

Approved Electronic Mail

Includes all mail systems supported by the IT Support Team. These include, but are not necessarily limited to, [insert Enterprise supported mailers here…]. If you have a business need to use other mailers contact the appropriate support organization, OTS Network Services

College Information System Resources

College Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above.

Expunge

To reliably erase or expunge data on a PC or Mac you must use a separate program to overwrite data, supplied as a part of Norton Utilities. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten. The same thing happens on UNIX machines, but data is much more difficult to retrieve on UNIX systems.

Individual Access Controls

Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On UNIX machines, this is accomplished by careful use of the chmod command (use *man chmod* to find out more about it). On Mac’s and PC's, this includes using passwords on screensavers, such as Disklock.

Insecure Internet Links

Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of W. L. Bonner College.

Encryption

Secure W. L. Bonner College Sensitive information in accordance with the *Acceptable Encryption Policy*. International issues regarding encryption are complex. Follow College guidelines on export controls on cryptography, and consult your manager and/or Enterprise legal services for further guidance.

Physical Security

Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.

Private Link

A Private Link is an electronic communications path that W. L. Bonner College has control over its entire distance. For example, all W. L. Bonner College networks are connected via a private link. A computer with modem connected via a standard land line (not cell phone) to another computer has established a private link. ISDN lines or cable to employee’s homes are a private link. W. L. Bonner College also may have established private links to selected organizations, so that all email correspondence can be sent in a more secure manner. Organizations that W. L. Bonner College has established such private links may include major constituency organizations and some short-term temporary links.

W. L. Bonner College

SECTION:	**RISK/AUDIT POLICIES**	**EFFECTIVE DATE: 7/1/2012**
SUBJECT:	**RISK ASSESSMENT POLICY**	**REVISED:**
POLICY #:	**RA-1**	**REVIEWED:**

RA-1 RISK ASSESSMENT POLICY:

1. Purpose

To empower the Office of technology Services (OTS) to perform periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

2. Scope

Risk assessments can be conducted on any entity within W. L. Bonner College or any outside entity that has signed a *Third Party Agreement* with W. L. Bonner College. RAs can be conducted on any information system, to include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

3. Policy

The execution, development and implementation of remediation programs is the joint responsibility of OTS and the department responsible for the systems area being assessed. Employees are expected to cooperate fully with any RA being conducted on systems for which they are held accountable. Employees are further expected to work with the OTS Risk Assessment Team in the development of a remediation plan.

4. Enforcement

Any employee found to have violated this policy might be subject to disciplinary action, up to and including termination of employment.

5. Definitions

Terms Definitions

Entity Any business unit, department, group, or third party, internal or external to W. L. Bonner College, responsible for maintaining W. L. Bonner College assets.

Risk Those factors that could affect confidentiality, availability, and integrity of W. L. Bonner College's key information assets and systems. OTS is responsible for ensuring the integrity, confidentiality, and availability of critical information and computing assets, while minimizing the impact of security procedures and policies upon business productivity.

W. L. Bonner College

SECTION:	**RISK/AUDIT POLICIES**	**EFFECTIVE DATE: 7/1/2012**
SUBJECT:	**AUDIT POLICY**	**REVISED:**
POLICY #:	**RA-2**	**REVIEWED:**

RA-2 AUDIT POLICY:

1. Purpose

To provide the authority for members of W. L. Bonner College's Office of Technology Services (OTS) team to conduct a security audit on any system at W. L. Bonner College.

Audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources
- Investigate possible security incidents ensure conformance to College security policies
- Monitor user or system activity where appropriate.

2. Scope

This policy covers all computer and communication devices owned or operated by the College. This policy also covers any computer and communications device that are present on College premises, but which may not be owned or operated by the College.

3. Policy

When requested, and for the purpose of performing an audit, any access needed will be provided to members of the College's OTS team.

This access may include:

- User level and/or system level access to any computing or communications device
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on College equipment or premises
- Access to work areas (labs, offices, cubicles, storage areas, etc.)
- Access to interactively monitor and log traffic on W. L. Bonner College networks.

4. Enforcement

Any employee found to have violated this policy might be subject to disciplinary action, up to and including termination of employment.