



September 16, 2010

DIVISION OF
INFORMATION
TECHNOLOGY

BSU STRATEGIC INFORMATION TECHNOLOGY SECURITY PLAN (DRAFT)

BSU Strategic Information Technology Security Plan (Version 1.0) |
Suresh Murugan - Information Systems Security Officer



BSU Security Plan for Information Systems | CONTENTS

Knowledge enablers	v
Executive Summary	1
1. Overview	2
A. Purpose.....	2
B. Audience	2
C. Document Organization	2
2. Security Mission and Vision.....	4
A. Security Mission.....	4
B. Security Vision.....	4
3. Security Weaknesses and Constraints	5
A. General Security Weaknesses	5
B. Business Continuity and Disaster Recovery.....	5
C. Privacy	5
D. Constraints	5
4. Threats and Vulnerability.....	7
5. Strategic Security Goals, Objectives, and Strategies.....	8
A. Goal 1: Improve Information Security Practices, Process, and Procedures	8
B. Goal 2: Provide enhanced and secure IT infrastructure for all campus-wide customers.....	9
C. Goal 3: Improve customer understanding of INFOSEC responsibilities.	10
D. Goal 4: Ensure that data stored on Bowie State University systems is secure, available and accurate.....	10
E. Goal 5: Ensure compliance with applicable federal, state, and local laws and regulations.	12
6. Conclusion	13





This page is intentionally blank for either a blank even page or the continuation of the Table of Contents.



Knowledge enablers

Knowledge Enablers are pictures that represent the tone and message of content. They are used in a table, as shown below.



Note

Alerts the reader to important text



Remember

Restates important information or procedures



Tip

Directs the reader's attention to a fact or hint



Warning

Alerts the reader to information that can avoid critical problems or errors



Advanced Knowledge

Designates information that is primarily of benefit to experienced readers



Geographic Dependency

Designates different information based upon a reader's geographic location





EXECUTIVE SUMMARY

Executive Summary

Bowie State University is an established HBCU located in Bowie, MD that strives to ensure a broad scope of knowledge and understanding that is deeply rooted in expanded research activities. Originally established in 1865, Bowie State University (BSU), through the effective and efficient management of its resources, provides high-quality and affordable educational opportunities at the baccalaureate, master's and doctoral levels.

Like many higher education organizations, the University must ensure that the students, faculty and administrators have access to the information resources required to maintain a functional learning environment. The key to such an environment this information is the availability of a campus network capable of providing the most reliable means of access securely.



1. Overview

Securing mission-critical University information and technology resources is crucial as accessibility to these resources for Bowie State University customer's increases. To protect its online resources, the University requires a comprehensive approach to securing these resources and addressing compliance. This includes strategies and mechanisms for preventing, detecting, and responding to security threats and attacks. There will be increased demands for continuous reliability as access to information is available anytime, anywhere.

A. Purpose

This plan defines a comprehensive program to secure and protect Bowie State University electronic information systems and data assets. The plan provides a framework of operational "best practices" that support all necessary components of information systems security required for the university to meet its compliance obligations to both federal and state regulations. Beyond mandatory compliance requirements, this plan is designed to support the university's own high standards and commitment to the preservation and protection of privacy, intellectual property, and quality technology-related services for all students, faculty, and staff who become involved with the institution.

B. Audience

Audience

Full Copy:

- NOC team
- BSU DIT Senior Management

Santized Copy:

- External LA Auditors team
- USM Internal Auditors team

C. Document Organization

Documentation sytem is organized as follows:

- Overview
- Security Mission and Vision
- Security Weaknesses and Constraints
- Threats and Vulnerability



OVERVIEW

- Strategic Security Goals, Objectives, and Strategies
- Conclusion



2. Security Mission and Vision

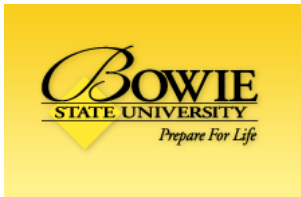
A. Security Mission

The objective of information security at Bowie State University is to protect information and data systems from unauthorized access, unauthorized modification or damage, or interruption to business functions. To accomplish this, Bowie State University information security mission is to provide timely, reliable, and cost effective security solutions for the protection and privacy of information owned by or entrusted to the university.

B. Security Vision

The security vision encompasses the following ideals:

- Empower our customers with obtaining critical real-time business information anytime and anywhere through a seamless and secure technology environment.
- Reduce risk of litigations and information disclosure through comprehensive policies, procedures and training.
- Strengthen our security posture through a combination of system hardening, segregation of sensitive systems, and enhanced perimeter security.
- Achieve and maintain full compliance to federal and state requirements by strong internal auditing.



3. Security Weaknesses and Constraints

A. General Security Weaknesses

The following weaknesses are current barriers to achieving the mission of an enterprise information security program:

- <Removed>.
- <Removed>.
- <Removed>.
- <Removed>.

B. Business Continuity and Disaster Recovery

- <Removed>.
- <Removed>.
- <Removed>.
-

C. Privacy

- <Removed>.
- <Removed>.
- <Removed>.
-

D. Constraints

In addition to the business objectives and initiatives driving security, there are also a range of constraints that inhibit or prevent the achievement of security objectives. These factors may be internal to the organization and controllable, or external and beyond the control of the organization.

Some external constraints are:

- <Removed>.
- <Removed>.
- <Removed>.
-
-



Some internal constraints are:

- <Removed>.
- <Removed>.
- <Removed>.
-

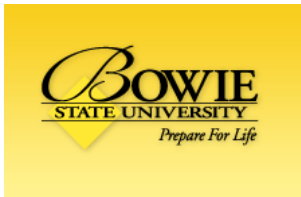
Any effective deployment of security strategies must allow for these constraining factors.

There are also some additional challenges to strategically planning implementation of security measures. Developing and implementing a successful strategic plan to properly protect its information systems resources and associated data involves an enormous set of challenges. They include:

- <Removed>.
- <Removed>.
- <Removed>.
-
-

This strategic plan takes into account the realities of what is involved. It assumes that if the university intends to reduce the incidents of intrusions, misuse of its computing resources and inappropriate access to data, resources will have to be allocated. The reality is that currently BSU does not have budgeted resources specifically for many of IT initiatives. This problem is compounded by the fact that, even with financial resources, finding the necessary expertise to support security efforts is difficult. Elements of this plan are defined in response to these realities.

This plan includes several immediate affordable steps as well as important long-term strategies to help grow a stronger awareness of and emphasis on security and privacy protection. In addition, the plan is designed around a risk management approach that includes documenting the cost of prevention verses the costs of potential incidences.



4. Threats and Vulnerability

There are several recognized Bowie State University IT security risks that must be addressed and resolved. These include:

- <Removed>.
- <Removed>.
- <Removed>.
- <Removed>.
-

Bowie State University also has some security issues as well:

- <Removed>.
- <Removed>.
- <Removed>.
- <Removed>.
-

Without addressing these concerns, there is the high probability of:

- <Removed>.
- <Removed>.
- <Removed>.
-

A poor enterprise security program will have several immediate, short term and long term affects on the university. The immediate economic impact on the university include: damage to systems that require extensive human intervention to repair or replace; disruption of administrative and academic operations; ad delays in transactions and cash flow. The short term economic impact to the university include: loss of contractual relationships with other organizations; loss of grants and other sources of funding; negative impact on reputation; hindrance to the development of new programs and funding; insurance recovery costs; regulatory fines and regulatory response; legal costs for forensics, depositions, and defense. Lastly, the long term economic impact on the university includes: increase insurance premiums; decline in alumni confidence; long term funding decline or interruption.

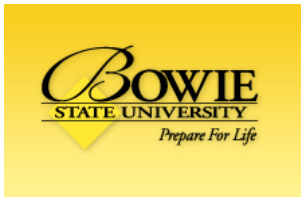


5. Strategic Security Goals, Objectives, and Strategies

This strategic IT security plan introduces a five year security program that introduces cost-effective security control solutions while balancing the university's need for open information exchange with controls that protect university systems and data. First and foremost is the use of a strategic architectural approach comprised of network-centric security, risk classification-based prioritization and zones of trust. These goals, objectives and strategies support the development and implementation of a uniform defensive multi-layered technical protection measures approach composed of prevention, detection and response. It is a living document that will be reviewed annually.

A. Goal 1: Improve Information Security Practices, Process, and Procedures

- Objective 1: <Removed>
 - Strategy 1 – <Removed>
 - Strategy 2 – <Removed>
 - Strategy 3 – <Removed>
- Objective 2: <Removed>
 - Strategy 1 – <Removed>
 - Strategy 2 – <Removed>
 - Strategy 3 – <Removed>
 - Strategy 4 – <Removed>
- Objective 3: <Removed>
 - Strategy 1 – <Removed>
 - Strategy 2 – <Removed>
 - Strategy 3 – <Removed>
- Objective 4: <Removed>
 - Strategy 1 – <Removed>
 - Strategy 2 – <Removed>
- Objective 5: <Removed>
 - Strategy 1 – <Removed>
 - Strategy 2 – <Removed>
 - Strategy 3 – <Removed>



STRATEGIC SECURITY GOALS, OBJECTIVES, AND STRATEGIES

- Objective 6: <Removed>
 - Strategy 1 – <Removed>
 - Strategy 2 – <Removed>
- Objective 7: <Removed>
- Objective 8: <Removed>

B. Goal 2: Provide enhanced and secure IT infrastructure for all campus-wide customers.

- Objective 1: <Removed>
 - Strategy 1 – <Removed>
 - Strategy 2 – <Removed>
 - Strategy 3 – <Removed>
 - Strategy 4 – <Removed>
- Objective 2: <Removed>
 - Strategy 1 – <Removed>
 - Strategy 2 – <Removed>
 - Strategy 3 – <Removed>
- Objective 3: <Removed>
 - Strategy 1 – <Removed>
 - Strategy 2 – <Removed>
- Objective 4: <Removed>
 - Strategy 1 – <Removed>
 - Strategy 2 – <Removed>
 - Strategy 3 – <Removed>
- Objective 5: <Removed>
 - Strategy 1 – <Removed>
 - Strategy 2 – <Removed>
- Objective 6: <Removed>
- Objective 7: <Removed>

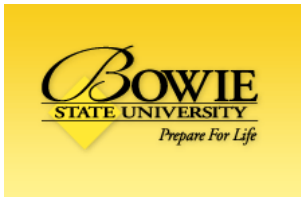


C. Goal 3: Improve customer understanding of INFOSEC responsibilities.

- Objective 1: <Removed>
 - Strategy 1 – <Removed>
 - Strategy 2 – <Removed>
 - Strategy 3 – <Removed>
 - Strategy 4 – <Removed>
- Objective 2: <Removed>
 - Strategy 1 – <Removed>
 - Strategy 2 – <Removed>
 - Strategy 3 – <Removed>
- Objective 3: <Removed>
 - Strategy 1 – <Removed>
 - Strategy 2 – <Removed>
 - Strategy 3 – <Removed>
 - Strategy 4 – <Removed>.
- Objective 4: <Removed>
 - Strategy 1 – <Removed>
 - Strategy 2 – <Removed>
 - Strategy 3 – <Removed>
- Objective 5: <Removed>
 - Strategy 1 – <Removed>
- Objective 6: <Removed>
 - Strategy 1 – <Removed>
 - Strategy 2 – <Removed>
 - Strategy 3 – <Removed>

D. Goal 4: Ensure that data stored on Bowie State University systems is secure, available and accurate.

- Objective 1: <Removed>
 - Strategy 1 – <Removed>



STRATEGIC SECURITY GOALS, OBJECTIVES, AND STRATEGIES

- Strategy 2 – <Removed>
- Strategy 3 – <Removed>
- Strategy 4 – <Removed>
- Strategy 5 – <Removed>
- Strategy 6 – <Removed>
- Strategy 7 – <Removed>
- Strategy 8 – <Removed>
- Objective 2: <Removed>
 - Strategy 1 – <Removed>
 - Strategy 2 – <Removed>
 - Strategy 3 – <Removed>
- Objective 3: <Removed>
 - Strategy 1 – <Removed>
 - Strategy 2 – <Removed>
 - Strategy 3 – <Removed>
 - Strategy 4 – <Removed>
 - Strategy 5 – <Removed>
 - Strategy 6 – <Removed>
 - Strategy 7 – <Removed>
- Objective 4: <Removed>
 - Strategy 1 – <Removed>
 - Strategy 2 – <Removed>
- Objective 5: <Removed>
 - Strategy 1 – <Removed>
 - Strategy 2 – <Removed>
 - Strategy 3 – <Removed>
- Objective 6: <Removed>
 - Strategy 1 – <Removed>
 - Strategy 2 – <Removed>
- Objective 7: <Removed>
 - Strategy 1 – <Removed>
 - Strategy 2 – <Removed>
- Objective 8: <Removed>



- Objective 9: <Removed>
 - Strategy 1 – <Removed>
 - Strategy 2 – <Removed>
 - Strategy 3 – <Removed>

E. Goal 5: Ensure compliance with applicable federal, state, and local laws and regulations.

- Objective 1: <Removed>
 - Strategy 1 – <Removed>
- Objective 2: <Removed>
 - Strategy 1 – <Removed>
 - Strategy 2 – <Removed>
 - Strategy 3 – <Removed>
- Objective 3: <Removed>
- Objective 4: <Removed>
 - Strategy 1 – <Removed>
 - Strategy 2 – <Removed>
 - Strategy 3 – <Removed>
 - Strategy 4 – <Removed>



6. Conclusion

Information security is first, and foremost, a cultural issue. Security cannot be bolted on but must be built into all our work and processes. Security must ultimately be a red button issue, just as structural safety is in building construction. Also one must think like the enemy in order to be able to defend against attacks.

While some areas of the Bowie State University INFOSEC infrastructure supported by the DIT Department are in good shape, other locations and areas are in need of substantial attention and investment of time and/or funding. This plan is to combine world-class best practices and leading edge security technology to support the academic mission of the University.

The DIT Department can not accomplish this strategic plan alone. It can only be achieved with input, involvement and commitment from all IT stakeholders of Bowie State University, and with cooperation and collaboration between the DIT Department and the other Bowie State University departments that provide IT support.