July 20, 2018

President Ava Parker
4200 Congress Avenue, MS 21,
AD 0210
Lake Worth, FL 33461
561.868.3501
parkera@palmbeachstate.edu

Dear President Parker,

The Florida College System, Chief Information Officers Council (FCS-CIO Council) is pleased to respectfully submit, on behalf of its membership, the enclosed whitepaper titled, Florida College System Cybersecurity Ecosystem*, to the Council of President's for review. The document was designed and unanimously approved by the membership of the Chief Information Officers Council and the associated security professionals within each institution. Presentations were given, and conceptual support received**, by the Councils of Business Officers, Instructional Affairs, and Student Affairs in spring, 2018.

The purpose of this document is to establish common, collectively supported frameworks, design principles and assumptions, and recommendations toward improved cyber security protocols. The foundational premise of the proposed cybersecurity ecosystem is that *every student in every college in the Florida system is afforded the same information security protections regardless of college size, resources, demographics, or location.*

The proliferation of cyber attacks requires a proactive approach that leverages the collaborative influence of the Florida College System in cyber security governance through the assessment, mitigation, and response. Guidance from the Florida Department of Education, State Board of Education, and the Auditor General's office suggests additional emphasis and prompts to the Council of Presidents on the topic of data and privacy protections and technological system security.

The FCS-CIO Council requests the following review and action:

1. Awareness, at the System level of the implications and recommended response to the current cyber vulnerabilities.
2. Approval of the Florida College System Cybersecurity Ecosystem Whitepaper.
3. Consideration of incorporating the establishment of a Florida College System Cybersecurity Ecosystem into the Council of President's legislative agenda, with funding provided to support the foundational premise noted above to collectively support a strengthened cybersecurity posture.
4. Charge the FCS-CIO Council with the tasks necessary to move forward in support of the six recommendations noted in the whitepaper, some of which will require additional funding to better secure infrastructure and operating process, and others which are operational in nature.

It would be our honor to present for the Council of Presidents and/or answer any questions that you might have as a result of this submission.

Respectfully submitted on behalf of the Florida College System CIO Council,

Florida College System, Chief Information Officer Council Co-Chairs

Naomi Boyer	Jason Dudley
Polk State College	Florida SouthWestern State College
nboyer@polk.edu	Jason.Dudley@fsw.edu

*The provided version has sensitive information regarding systems utilized in each College removed but can be made available upon request through secure transfer.
**Letter of endorsement provided by CIA/CSA groups

SPRING
2018

Florida College System Cybersecurity Ecosystem

DEVELOPING AN INFORMATION SECURITY ECOSYSTEM FOR THE FLORIDA COLLEGE SYSTEM

FLORIDA COLLEGE SYSTEM, CIO COUNCIL, APPROVED 4/30/18

The enclosed document is respectfully submitted on behalf of the Florida College System CIO Council and represents contributions from Council members and the associated security professionals from the member institutions.

Executive Summary

Information security and cybersecurity have become critical risk issues for all organizations, particularly those in the education sector. It is not overstating to suggest that technological vulnerabilities have the potential to cause significant harm to the students we serve, the faculty and staff we employ, and result in excessive financial impacts to our colleges. A recent Florida-based example demonstrates the importance and need for coordinated response:

> In early January 2018, many Florida college and university presidents received a threat email that blurred the lines between cyber threat, extortion, physical safety, and security. The widespread nature of the email campaign engaged law enforcement, including the FBI, and forced local action in anticipation of possible violence.

Unfortunately, the proliferation of these types of incidents have demanded increased attention and targeted response. The Florida College System Chief Information Officer (CIO) Council presents this white paper as a proactive attempt to define an ecosystem that unifies implementation approaches, maximizes resources and purchasing efficiencies, advocates for institutional and state level support, forges a network of relationships to augment efforts, and cultivates a shared understanding of information security.

Through the use of a collaborative design approach and a shared working theory, we leveraged industry frameworks and focused on critical controls to establish a foundation for Florida College System institutions. Communication between institutions is critical to ensure that *every student in every college in the Florida system is afforded the same information security protections regardless of college size, resources, demographics, or location.* These communication channels are essential to support the ecosystem of schools, while also aligning to each institution's posture to existing threats or incidents.

Design Principles

1. Design utilizing existing frameworks (ex: NIST) and standards.
2. Incorporate strategies that align to cybersecurity insurance criteria to minimize exposure.
3. Compliance and mandates provide the minimum expectation rather than the optimal state.
4. Recommend and implement solutions that leverage economies of scale to optimize deployment across the college system.
5. Establish shared resource development options (potential legislative support) and collective advocacy to provide mechanisms for sustainable solutions.
6. Recognize the unique characteristics of individual college identities, processes, and analyses.

Recommendations

5.1 Adopt NIST Cybersecurity Framework.
5.2 Utilize a common assessment tool.
5.3 Begin with the CIS Critical Security Controls Top 20.
5.4 Develop a common incident response procedure.
5.5 Establish a Florida College System Information Security Officers Group (FCS-ISO).
5.6 Develop a communication protocol and an Alert approach between Colleges.

To this end, six design principles and recommendations have been identified and collectively supported by the Florida College System CIO Council and the associated information security officers within the participating institutions. Additional details are provided regarding each of the design principles (section 3) and recommendations (section 5) within the document. The principles and recommendations align with and support the many compliance and audit control documents that govern and protect our business processes and technological environments.

To support these recommendations, a dedicated funding stream would best facilitate consistent adoption of best practice IT Security principles across all FCS institutions. An analysis to determine potential costs and a possible funding mechanism would be developed by a collaborative effort between the FCS-CIO's with guidance from the Council of Presidents. System-level funding sources will be utilized to establish and sustain the noted recommendations and associated necessary personnel, processes, and technical infrastructure at FCS institutions.

Florida College System Cybersecurity Ecosystem

Developing an information security ecosystem for the Florida College System

1 INTRODUCTION

Information technology (IT) organizations throughout the state of Florida provide capabilities to institutions in support of their mission. One of these capabilities is the safeguarding of institutional information from improper use. Given the proliferation of data breaches, insidious ransomware, phishing, malware attacks, and identity/privacy fraud that have spread across all industries including higher education, the Florida College System (FCS) recommends a targeted proactive approach to the assessment, mitigation, and response process. Ultimately, it is not a matter of if a risk or vulnerability will occur, but more fundamentally accepting the likelihood that it will occur. Adopting and implementing a comprehensive approach to information security will minimize the impact of the risks and provide for a more effective approach to incident response.

In September 2011, the FCS and College Center for Library Automation (CCLA) CIOs developed a set of common guidelines designed to establish minimum, ideal goal objectives for the security maturity postures of both systems. However, over the last seven years, the topic of cybersecurity has become even more critical to our institutions, and earlier guidelines have become out dated.

This white paper addresses the need for an updated, more robust set of standards. It defines an ecosystem that unifies implementation approaches, maximizes resources and purchasing efficiencies, advocates for institutional- and state-level support, forges a network of relationships to augment efforts, and cultivates a shared understanding of information security. The ultimate goal is to provide “the what” of what cybersecurity measures are in practice and are recommended for ultimate protection and “the how” of

how Florida College System institutions can join together to improve the overarching cybersecurity ecosystem, regardless of college size, demographic, or location. This is not intended to be a mandate; the provided recommendations are offered with the understanding that the "who" and "when" questions must be answered within each educational institution based upon personnel and fiscal resources, culture, and risk tolerance.

2 DEFINING THE APPROACH

The Florida College System Chief Information Officer Council (FCS-CIO) has met regularly to discuss common issues, participate in professional development, and share progress and practices. Over the last five years, the topic of cyber security has become critical to the technological and organizational health of the individual organizations and the collective. Of great concern to the membership is not only establishing independent protective structures, but also shoring up our connective and cooperative partnerships to ensure that all Florida colleges have access to a network of technological, financial, project, and human resources to manage change and respond to emergent threats. It is worthwhile to note that having a system that provides total and complete protection is not possible. Our goal is to implement a sustainable program that balances the need to protect information resources against the need to run business operations. Although it is true that security controls cannot mitigate every threat, we know that properly implemented security controls can minimize the impact of an incident and provide a level of readiness during a security incident response.

Based upon the landscape of existing frameworks provided by industry leaders, current practices within each of the participating colleges, and trends in security processes and tools, the group engaged in preliminary surveys, literature and resource review, design workshops, and collective composition. Cyber security and information protection have been identified as areas of focus for senior leadership throughout higher education. EDUCAUSE has identified security (information and compliance) as a Top 10 IT Issue for the last 10 years, with 2012 being the only year in the last decade that these critical issues were not listed. More recently, the number one leading issue noted in the 2018 EDUCAUSE Review (2018) is "Information Security: Developing a risk-based security that keeps pace with security threats and challenges" (pg. 12).

Every Student in every college in the Florida system is afforded the same information security protections regardless of college size, resources, demographics or location

The topics of threat assessment, threat mitigation, and incident response provide the structure for this document. It should be noted that while the work sessions included confidential data, only aggregated information is presented to not expose any of the participating members to greater vulnerability.

3 Design Principles

As previously noted, the working theory of the FSC-CIO council is: every student in every college in the Florida system is afforded the same information security protections regardless of college size, resources, demographics, or location.

With the basis of this working theory, several design principles were defined to guide the development of a shared information security framework:

1. Design utilizing existing frameworks (ex: NIST) and standards.
2. Incorporate strategies that align to cybersecurity insurance criteria to minimize exposure.
3. Compliance and mandates provide the minimum expectation rather than the optimal state.
4. Recommend and implement solutions that leverage economies of scale to optimize deployment across the college system.
5. Establish shared resource development options (potential legislative support) and collective advocacy to provide mechanisms for sustainable solutions.
6. Recognize the independent and local control of individual institutions while leveraging the unique characteristics of each institutions individual identity, processes and analyses.

Uniting for Individual Defense

In both nature and politics, it is very important to get the balance right between individual ecosystems and the larger whole, so each can nurture the other.

Thomas L. Friedman. (2016). Thank You For Being Late: An Optimist's Guide to Thriving in the Age of Acceleration.

A college's individual identity should in no way negate the safeguards that are established. Therefore, the following elements provide the opportunity to build shared vocabularies, strategies, and efficiencies to maximize systemic support:

- Establish a Network of College Security Professionals. The most efficient and effective source of information can be found in the network of talented cyber security experts within the Florida College System. Through existing resources, a variety of tools can be deployed to share information and collaborate on best practices. A listserv, access to a shared content repository,

and a schedule of regular meetings via electronic and face-to-face means will be implemented to facilitate a vibrant network of relationships.

- **L**everage economies of scale in order to maximize the fiscal resources of the Florida College System and the individual colleges; efforts can be unified to extend buying power. Some examples include:
    1. Consortium negotiation on security products such as services, hardware, and software/applications aligned to assessment gaps and mitigation needs.
    2. Bulk registration for security professional development opportunities such as conferences, webinar series, workshops, and trainings.
    3. Partnership agreements to reduce association, organization, service vendor (i.e. Gartner, etc.), and subscription costs.
- **D**efine a dedicated funding source to support institutions in remaining hardening cyber-infrastructure, engaging cyber incident management and response services, establishing and sustaining personnel training and awareness capabilities, reacting to changing data privacy and protection regulations and hiring qualified information security personnel throughout the system.

An unfortunate reality in the technology market is that the tools to mitigate and respond, when necessary, require significant organizational resources. There are tools that can be applied to fortify human practices to assist with log analysis, network protection, viral infiltration, web protections, email attacks, and many others; however, due to funding issues, some of the colleges remain more exposed than others.

Each individual institution believes that information security should be integrated into each project and program to enhance and enable information technology capabilities within the institution, and independent programs should be focused on information security concerns. This belief requires integration into financial budgeting, technology management, and release and configuration management. These individual plans and processes will be shared with the collective FCS institutions to gather any economies of scale and leverage shared purchasing power.

3.1 Governance Models

The integral and fundamental role of information technology in communications, academics, and business operations necessitates governance plans that strategically address mission-critical business challenges, adequate risk management, and institutional reporting and accountability. Information technology governance is not just an issue relegated to the offices that support technology; rather, it is a responsibility shouldered by all executive leaders and boards to incorporate effective information technology governance practice to ensure quality assurance and organizational alignment of technology to institutional decision making about business/academic objectives.

Effective information technology governance supports academic and business goals, optimizes and justifies investment in technology, and appropriately manages information technology-related risks and opportunities. Any cybersecurity posture should be a portion of the overarching formalized information technology governance processes established by executive leaders. These implemented governance processes allow for appropriate resource allocation, prioritization of effort, and critical assessment of institutional risk appetite that will ultimately guide decision making on cyber security tactics.

The recommendation and collective agreement on information technology governance processes and frameworks will be vital to the ongoing assessment, mitigation, and response approaches. The use of current information technology governance frameworks, such as Control Objectives for IT 5 (COBIT 5), IT Infrastructure Library (ITIL), and Factor Analysis of Information Risk (FAIR), can help the state colleges utilize governance in a manner that aligns to the unique college identities and help to unify the cyber security protection mechanisms of scale to support broad implementation and funding. Establishing recommendations for governance at the Florida College System and institutional level will fall to the network of Florida College System Security Officers Group. These governance models support a culture of information technology governance, engagement, and decision making and guide the implementation of security frameworks.

4 DEFINING AN INFORMATION SECURITY SOLUTION FOR FCS INSTITUTIONS

Within the domain of information security, there are several bodies of knowledge that have established frameworks, structures, and standards. The FCS-CIO Council commissioned a review of several of these frameworks, and the Florida College Information Security Officers (FCISO) working team was tasked with developing a framework and set of activities that would enable leadership at each College to deliver on the working theory that every student in every college in the Florida system is afforded the same information security protections regardless of college size, resources, demographics, or location. The challenge was to find a standard approach that meets these goals, while also allowing flexibility to account for the unique culture and needs of each institution. A common approach to assessing each institution's information security program would be needed, utilizing a common language and approach to convey its views and approach to cybersecurity risks. This approach goes beyond the adoption of controls to address or mitigate cybersecurity risks. The need was for a common set of outcomes and activities, yet allowing for flexibility with how these were conducted and achieved.

Also informing the recommendations from the FCISO working team was guidance from the Florida Agency for State Technology (AST) that published the Statewide Information Technology Security Plan in February 2015. It provides technology guidance for 32 executive branch agencies. It contains three arguably aggressive strategies: (1) Enhance security and privacy capabilities, (2) Enhance the enterprise IT environment, and (3) Define the roadmap for maturing IT processes and strategic business alignment. It is a living document, which includes a "roadmap" for future development. The Florida Cybersecurity Standards (FCS) went into effect in March 2015 with the initial statewide risk assessment occurring in June 2015. Chapter 74-2 of the Florida Administrative Code was later released in March 2016, which was largely based on the National Institute of Standards and Technology's Cybersecurity Framework.

The NIST Cybersecurity Framework was developed to reduce cyber risks to the critical infrastructure per Executive Order 13636 (EO), "Improving Critical Infrastructure Cybersecurity," signed by President Barack Obama on February 13, 2013. As directed in the EO, the Cybersecurity Framework should include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks (Obama, 2013).

The current version of the NIST Cybersecurity Framework is the result of 10 months of collaborative discussions with more than 3,000 security professionals. The set of risk-based guidelines was designed to aid organizations from various industries identify, implement, and improve cybersecurity practices, and creates a common language for internal and external communication of cybersecurity issues (Guinn, II, et al., 2014). Although the framework is relatively new, the standards or concepts outlined in it are not. NIST fundamentally leveraged and integrated industry-leading cybersecurity practices that were developed by itself and the International Standardization Organization (ISO) (Guinn, II, et al., 2014). While the framework was originally aimed at organizations related to critical infrastructure, the cybersecurity community thought the adoption of the framework would be beneficial across virtually all industries, including education (Guinn, II, et al., 2014).

Based on a rigorous analysis of available frameworks and guidance from the State of Florida, the FCISO working team endorses the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (1.0), initially published in 2014 in response to an executive order to establish a set of standards for appropriately addressing the cybersecurity risks for organizations that comprise the critical infrastructure.

Although the Framework chosen allows for flexibility on the specific control catalog or standards to use to arrive to each outcome or rigor with which these controls would be applied, the working group did think that there should be a **standard baseline of controls** that would be both applicable and beneficial

for all colleges. This baseline provided by the Center for Internet Security (CIS) Critical Security Controls (CSC) for Effective Cyber Defense is also referred to as the CIS CSC Top 20[1]. These twenty controls were chosen by a cross-section of cybersecurity professionals in a wide range of industries as a risk-based set of controls that would be most effective to address the top threats that most institutions face. These controls consist mainly of technical and operational controls that map to specific outcomes of the Framework, which when implemented successfully along with additional administrative controls, provide each college with a sound baseline for its individual cybersecurity program.

The compilation of **collaborative design**, a shared **working theory**, leveraging **industry frameworks**, and focusing on **critical controls** will establish the foundation for FCS institutions. **Communication** between institutions is critical to define communication channels between FCS institutions in times of incident response. These communication channels will be utilized to share each institutions posture to existing threats or incidents.

5 RECOMMENDATIONS

The Florida College System Chief Information Officer Council (FCS-CIO) endorses the following recommendations establishing a baseline information security ecosystem:

5.1 OPTIMAL SET OF OUTCOMES BY ADOPTING THE NIST CSF

The NIST CSF is comprised of the following three components: Framework Core, Framework Implementation Tiers, and Framework Profile.[2]

[1] Center for Internet Security Critical Security Controls for Effective Cyber Defense. https://www.cisecurity.org/controls/

[2] Source: Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, NIST, February 12, 2014. Obtained from: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

- The Framework Core is a set of outcomes, activities, and informational references. At the highest level, the Core consists of five "concurrent and continuous" functions: Identify, Protect, Detect, Respond, and Recovery. Each function consists of a set of outcomes and activities that are grouped under categories and sub-categories, with additional information references for each sub-category intended to provide specific guidance based on popular controls' standards.
- The Framework Implementation Tiers provide the mechanism for an organization to describe its cybersecurity practices.
- The Framework also provides the mechanism to develop institutional cyber security profiles to indicate how the organization is aligned and desires to align with the categories and subcategories from the Framework Core.

5.2 Utilize NIST FCS Assessment Spreadsheet

The FCS Assessment Spreadsheet is founded on the cyber security assessment used by the State of Florida. The assessment is designed to gauge the institutions preparedness to mitigate cyber risks. NIST defines cyber security as "the process of protecting information by preventing, detecting, and responding to cyber-attacks." All institutions should consider managing internal and external threats, vulnerabilities to defend infrastructure, and information assets.

The FCS Assessments' intended use is for benchmarking an institution's cyber security preparedness as a baseline "minimum" standard. This assessment is designed to provide a measurable and repeatable process to assess an institution's level of cyber security risk and preparedness. The initial assessment will identify the institution's inherent risk relevant to cyber security. Secondly, the assessment will determine the institution's current state of cyber security, which will be represented in the four levels (bar graphs) represented across the top of each category. In order for this assessment to be an effective

risk management tool, an institution may want to complete the assessment periodically or when significant operational and technological changes occur.

The FCS Assessment factors are as follows:

Security Functions	Assessment Factors	Rule Chapter ID
Identify	Asset Management, Business Environment, Governance, Risk Assessment, Risk Management Strategy	FCS 74-2.002
Protect	Access control, Awareness & Training, Data Security, Information Protection, Maintenance, Protective Technology	FCS 74-2.003
Detect	Anomalies and Events, Continuous Monitoring, Detection Processes	FCS 74-2.004
Respond	Response Planning, Communications, Analysis, Mitigation, Improvements	FCS 74-2.005
Recover	Recovery Planning, Improvements, Communications	FCS 74-2.006

Institutional cyber security programs build upon and align with existing information security, business continuity, and disaster recovery guidelines. This FCS assessment will demonstrate where each security control feature aligns with the institution's policies, procedures, and guidelines.

5.3 Focus on the CSC Top 20

The Center for Internet Security (CIS) Top 20 Critical Security Controls (previously known as the SANS Top 20 Critical Security Controls) is a prioritized set of best practices created to stop the most pervasive and dangerous threats of today. The 20 Critical Security Controls were developed by leading security experts from around the world and are refined and validated every year. The Florida College System

Security Officers have elected to work towards complying with the CIS's Top 20 Critical Security Controls, starting with the first five, in an effort to protect our institutions from some of the most common attacks.

The first five Controls essentially focus on the basics to prevent disruptive attacks, including configuration management, vulnerability assessment, and continuous monitoring to know when a new critical vulnerability surfaces or an asset becomes exposed to reduce risk while adapting to both changing threats and changing business demands.

1. Inventory devices
2. Inventory software
3. Secure configuration
4. Vulnerability assessment
5. Local admin

Appendix 7.4 will provide an example of implemented solutions that some member institutions have utilized to mitigate vulnerability and satisfy the first five controls.

5.4 Incident Response Procedures

The first five controls within the CIS CSC Top 20 enable effective management of cybersecurity risks by identifying the components to protect and the opportunities for applying controls. In addition to the first five of the CIS CSC Top 20, establishing an incident response process would enable each college to effectively handle incidents for those assets (hardware, software, and data), threats, and vulnerabilities not protected by other controls. This recommendation addresses the control objectives under the CIS CSC Incident Response and Management control (number 19 on the list of controls) by establishing standard components of an incident response procedure for each college to incorporate into its individual plans.

Incidents, in the context of cybersecurity, is defined by NIST as “an assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.”[3]

The capabilities necessary to effectively respond to and recover from incidents involve a wide range of activities from each of the Core Functions of the NIST CSF. These activities include the development, testing, and effective execution of response plans. To frame the response plan, and in keeping with the design principles for this initiative to leverage existing frameworks, standards and best practices, the working committee has chosen to follow the tactical guidelines from the NIST Special Publication 800-61 Revision 1, “Computer Security Incident Handling Guide.”[4] The guide provides a solid methodology for effectively handling response and recovery from adverse cybersecurity events.

The incident response lifecycle described by NIST consists of four main phases, providing a structured methodology to ensure consistency with each incident addressed. The following figure illustrates how these phases interact.

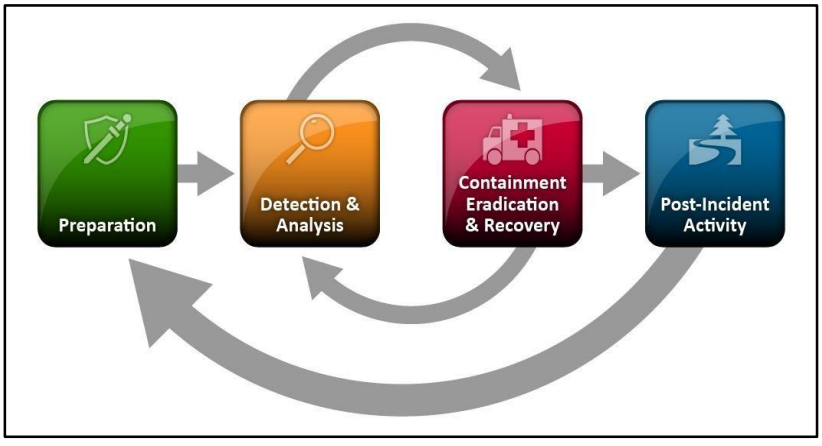


Figure 1: Incident Response Life Cycle, NIST SP 800-61 R2

[3] https://csrc.nist.gov/Glossary/?term=3545
[4] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

These four phases are used to develop the incident response procedures that provide steps for responding to the majority of potential cybersecurity incidents that the colleges can reasonably expect to face at some point. In addition to this white paper, the group has developed an incident response runbook, based on the NIST guide that describes the procedures to follow throughout the four phases. A checklist of the key steps to follow during an incident response, as adopted from the NIST SP 800-61 guide, are provided as Appendix 7.5.

5.5 Florida College System Information Security Officers Group (FCS-ISO)

- The primary function of the FC-ISO group is to collaborate from a strategic perspective pertaining to IT security management, design, oversight, and assessment.
- The domains of focus for the group include Information Security Governance, Information Risk and Compliance, Information Security Program Development and Management, and Incident Management.
- The FC-ISO group will function at the management level, working closely with the FC-CIO group to prioritize initiatives.
- The group will meet regularly to collaboratively plan and share information.
- The group will identify, recommend, and prioritize potential administrative, physical, and technical controls to satisfy strategic objectives.
- Subcommittees will be formed to address specific tactical recommendations or perform collaborative assessments or proof of concept testing.
- Subcommittees may include various operational technical staff, system admins, managers, ISOs, CIOs, and others.

5.5.1 Action Items:

- CIO and executive-level endorsement and support of the FC-ISO group.

- Determine meeting structure and frequency group (chairperson, vice-chairperson).

5.6 DEVELOP A COMMUNICATION PROTOCOL AND AN ALERT APPROACH BETWEEN COLLEGES

As with the national security alert systems, the establishment of a graduated scale security threat level (e.g. Low, Med, High; Red, Yellow, Green) is recommended. These levels would be distributed and published for all FCS institutions indicating a security posture of operation. Defined communication and NIST standard alignment would be required through common procedures and protocols. In addition, based on the identified system threat level, levels of communication will be recommended between institutions through secure channels. The sanctity and individuality of each institution is a basic tenant of the protocol and alert system, which empowers each college to respond as is locally appropriate. The threat level merely provides a standard barometer to assist in the assessment, mitigation, and response and facilitates system coordination of action.

5.6.1 Action Items:

- Establish a graduated scale security threat level that can be adopted by all of Florida College System colleges as a means of shared communication.
- Design a protocol for issuing an alert and strategies for response that provide a consistent understanding of action despite local alignment to emergency process.
- Leverage the existing FCS Chief Information Security Officer technical expertise available to develop a common vocabulary and system response to facilitate swift, yet secure, system-wide actions to cross-institutional threats.

6 REFERENCE LIST

2017 Florida Statutes. (2017). *K-20 Education Code, Public Postsecondary Education, 1004.055: Security of data and information technology in state postsecondary education institutions.* Retrieved from http://leg.state.fl.us/Statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=1000-1099/1004/Sections/1004.055.html

2017 Florida Statutes. (2017). *Florida: Public Business, Communications and Data Processing, 282.318: Security of data and information technology*. Retrieved from http://www.leg.state.fl.us/statutes/index.cfm?mode=View%20Statutes&SubMenu=1&App_mode=Display_Statute&Search_String=Security+of+data+and+information+technology.&URL=0200-0299/0282/Sections/0282.318.htmll

Association of Modern Technology Professionals. (2018). *Information Technology Infrastructure Library.* Retrieved from http://www.itinfo.am/eng/information-technology-infrastructure-library-guide/

Center for Internet Security. (n.d.). *CIS Controls*. Retrieved from https://www.cisecurity.org/controls/

EDUCAUSE Review. Retrieved from https://er.educause.edu/

FAIR Institute. (n.d.). What is FAIR. Retrieved from https://www.fairinstitute.org/what-is-fair

Florida Administrative Code & Florida Administrative Register. (2016). Florida, Rule Chapter: 74-2, Information Technology Security. Retrieved from https://www.flrules.org/gateway/ChapterHome.asp?Chapter=74-2

Florida Agency for State Technology. (n.d.). https://www.ast.myflorida.com/cybersecurity-updates/

Florida House of Representatives. (2017). HB 501: Public Records and Meetings/Information Technology/Postsecondary Education Institutions. Retrieved from http://laws.flrules.org/2017/109

Friedman, T. (2016). *Thank you for being late: An optimist's guide to thriving in the age of accelerations.* New York, NY: Farrar, Straus and Giroux.

Grajek, S. & the 2017-2018 EDUCAUSE IT Issues Panel. (2018). Top 10 IT Issues 2018: The Remaking of Higher Education. *EDUCAUSE Review*, *53 (1)*, 10-59.

Guinn, II, J., Burg, D., Compton, M., Harries, P., Hunt, J., Lobel, M., Loveland, G., Nocera, J., Roath, D. (2014, May). *Why you should adopt the NIST Cybersecurity Framework*. Retrieved from PwC: https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf

Information Technology Laboratory. (n.d.). *Computer Security Resource Center. Glossary.* Retrieved from https://csrc.nist.gov/Glossary/?term=3545

Joint Task Force Transformation Initiative. (2013). *National Institute of Standards and Technology Special Publication 800-53, Revision 4*. Retrieved from http://dx.doi.org/10.6028/NIST.SP.800-53r4

Martin, A. (2018, January). UCF settles massive computer hacking case. *Orlando Sentinel*. Retrieved from http://www.orlandosentinel.com/features/education/school-zone/os-ucf-hack-suit-20180111-story.html

McNeill, C. (2018, January). Extortion emails target Florida colleges, promising violence. *Tampa Bay Times.* Retrieved from http://www.tampabay.com/news/education/college/Extortion-emails-target-Florida-colleges-promising-violence_164167410

National Institute of Standards and Technology. U.S. Department of Commerce. (2012). *Computer Security Incident Handling Guide*. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

National Institute of Standards and Technology. (2014). Framework for Improving Critical Infrastructure Cybersecurity. Retrieved from https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

Obama, B. (2013). *Executive Order -- Improving Critical Infrastructure Cybersecurity. https*://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

PCI Security Standards Council. (n.d.). PCI SSC Data Security Standards Overview. Retrieved from https://www.pcisecuritystandards.org/pci_security/standards_overview

One Hundred Eleventh Congress of the United States (2010). *Red Flag Program Clarification Act of 2010, S.3987 - 111th Congress (2009-2010).* Retrieved from http://www.gpo.gov/fdsys/pkg/BILLS-111s3987enr/pdf/BILLS-111s3987enr.pdf

Systems Audit and Control Association (ISACA). (n.d.). *Control Objectives for IT 5* (COBIT 5). Retrieved from https://cobitonline.isaca.org/

U.S. Department of Education. (2015). *Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; 34 CFR Part 99*. Retrieved from https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

United States Government Accountability Office. (2009). Federal Information System Controls Audit Manual (FISCAM). Retrieved from http://www.gao.gov/new.items/d09232g.pdf

7 APPENDIX

Contents

7 Appendix 19
7.1 Information Security Standards – Aligned to Florida IT Audit 19
7.2 Information Security – Federal and Florida State Statues 21
7.3 CIS CSC Top 20 23
7.4 CIS CSC Top 5 Controls with Examples provided by Specific FCS Colleges. 24
7.5 Incident Handling Checklist (Post Event Occurrence) 29
7.6 Florida College System CIO Threat Mitigation Survey: Tools and Techniques 30
7.7 FCS Assessment Spreadsheet 31

7.1 INFORMATION SECURITY STANDARDS – ALIGNED TO FLORIDA IT AUDIT

Organization	Specific Standards	Comments
National Insitute of Standards and Technology (NIST): Information Technology Laboratory	NIST SP 800-53 Revision 4 Recommended Security and Privacy Controls for Federal Information Systems and Organizations NIST Cybersecurity Framework	Supported by the FCS-CIO group as the primary reference framework*. Source for the State of Florida Auditor General: **Information Technology Audit criteria presented at 2015 FAEDS Conference**

NIST SP 800 Specific framework alignment items to State of Florida IT audit

Risk Assessment

SP 800-53 Rev. 4 Security and Privacy Controls for Federal Information Systems and Organizations

SP 800-53 A Rev. 4 Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans

SP 800-137 Information Security Continuous Monitoring for Federal Information Systems and Organizations

SP 800-39 Managing Information Security Risk: Organization, Mission, and Information System View

SP 800-37 Rev. 1 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach

SP 800-30 Rev. 1 Guide for Conducting Risk Assessments

Data Loss Prevention

SP 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

SP 800-124 Rev. 1 Guidelines for Managing the Security of Mobile Devices in the Enterprise

SP 800-88 Rev. 1 Guidelines for Media Sanitization

Incident Response

SP 800-61 Rev. 2 Computer Security Incident Handling Guide

SP 800-83 Rev. 1 Guide to Malware Incident Prevention and Handling for Desktops and Laptops

Authentication Parameters

SP 800-70 Rev. 2 defines the National Checklist Program:

U.S. Government repository of publicly available security checklists for detailed low-level guidance on setting security configurations for operating systems and applications (includes password parameters).

Organization	Specific Standards	Comments
U.S. Government Accountability Office (GAO)	Federal Information System Controls Audit Manual (FISCAM)	State of Florida Auditor General: Information Technology Audit criteria

FISCAM Specific framework alignment items to State of Florida IT audit

Authentication Parameters

Protecting confidentiality of passwords as follows:

Individual users are uniquely identified rather than having users within a group share the same ID or password; generic user IDs and passwords should not be used.

Passwords are changed periodically, about every 30 to 90 days. The more sensitive the data or the function, the more frequently passwords should be changed.

Passwords are not displayed when they are entered.

Passwords contain alpha-numeric and special characters and do not use names or words that can be easily guessed or identified using a password-cracking mechanism.

A minimum character length, at least 8 characters, is set for passwords so that they cannot be easily guessed.

Use of old passwords (e.g., within 6 generations) is prohibited.

To help ensure that passwords cannot be guessed, attempts to log on to the system with invalid passwords should be limited (typically, potential users are allowed 3 to 7 attempts to log on).

Organization	Specific Standards	Comments
ISACA and the IT Governance Institute	Control Objectives for Information and related Technology (COBIT)	State of Florida Auditor General: Information Technology Audit criteria

ISACA Specific framework alignment items to State of Florida IT audit

Authentication Parameters

Protecting the confidentiality of passwords as follows:

User identification codes (user IDs) should be restricted to provide individual identification.

If the wrong password is entered a predefined number of times, typically 3, the user ID should be automatically locked.

Passwords are not displayed when they are entered and should be one-way encrypted internally.

Passwords should be a minimum of 8 characters.

Passwords should require a combination of a least 3 of the following: alpha-numeric, upper and lower case, and special characters.

The system should enforce regular password changes every 30 days and not permit previous password(s) to be used for at least a year.

Organization	Specific Standards	Comments

PCI Security Standards Council	PCI SSC Data Security Standards Overview	Recognized payment card data security.

Table 1. Security frameworks and standards used as criteria for Florida College System compliance review

*Note Appendix X of FCS-CIO Assessment review document aligned to SP 800-53, originally prepared by Florida State College and modified by Broward College. Submitted to the FCS-CIO for review and feedback.

7.2 Information Security – Federal and Florida State Statues

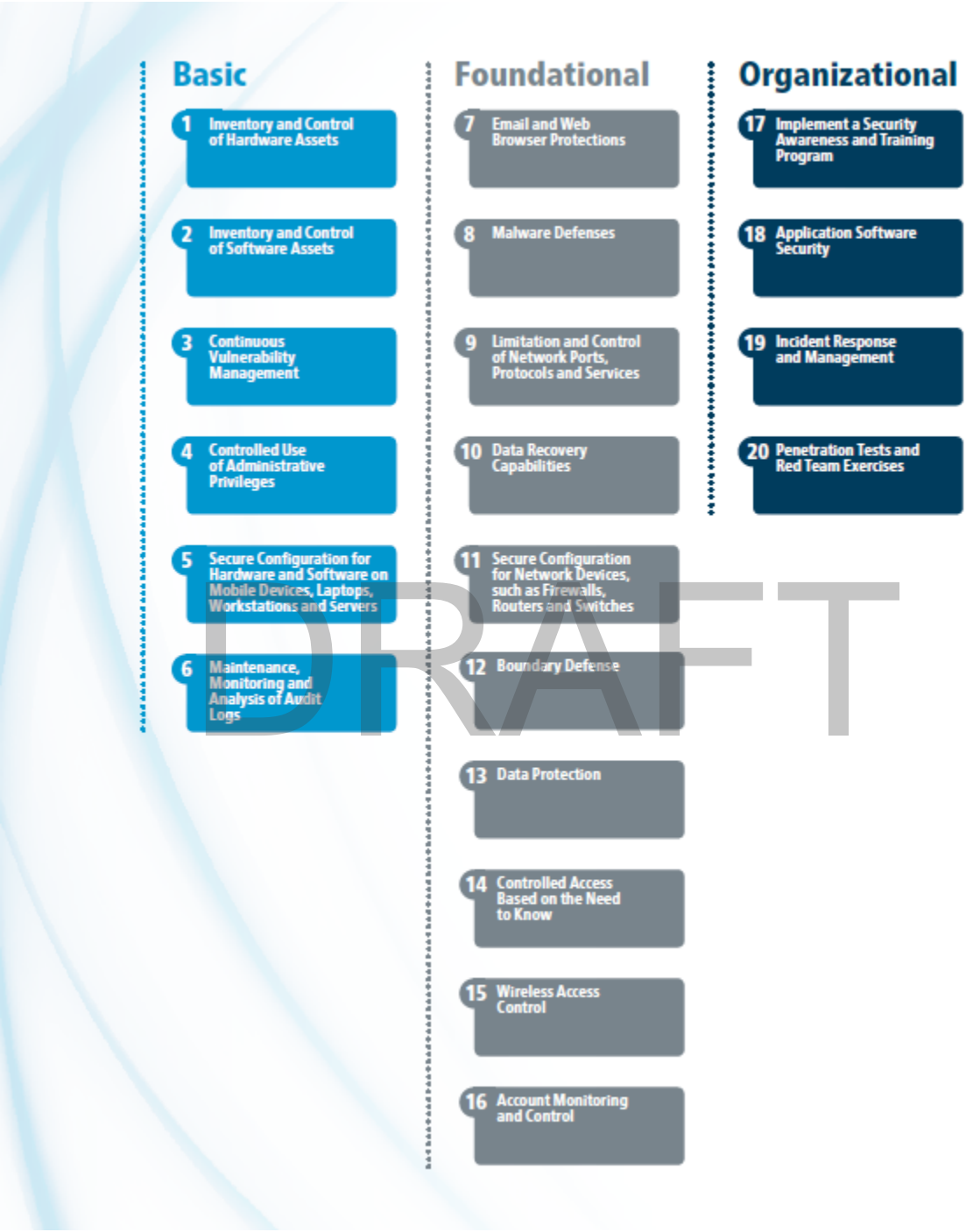
In addition to the noted frameworks, there are a number of compliance requirements and Florida State Statutes (Table 2) that pertain to data and information security and associated topics that must be utilized as a minimal threshold for the review and recommendation that follows in this document.

Law, Statute, & Administrative Code	**Title and Link**	**Federal/Florida**
20 U.S.C. § 1232g; 34 CFR Part 99	Family Educational Rights and Privacy Act (FERPA)	Federal
S.3987 - 111th Congress (2009-2010)	Red Flag Program Clarification Act of 2010	Federal
Federal Trade Commission, 16 CFR Part 314	Gramm-Leach-Bliley Act (GLBA): Safeguards Rule	Federal
Federal Student Aid alignment to GLBA Safeguards Rule	Federal Student Aid (FSA) Program Participation Agreement (PPA) Student Aid Internet Gateway (SAIG) Agreement	Federal
Federal Student Aid	DCL ID: Gen 15-18 DCL ID: Gen 16-12	Federal
EU General Data Protection Regulation (GDPR)	Directive 95/46/EC	International
FLORIDA: K-20 EDUCATION CODE, PUBLIC POSTSECONDARY EDUCATION, 1004.055	Security of data and information technology in state postsecondary education institutions	Florida
FLORIDA: PUBLIC BUSINESS, COMMUNICATIONS AND DATA PROCESSING, 282.318	Security of data and information technology	Florida
FLORIDA: K-20 EDUCATION CODE, K-20 GOVERNANCE, 1001.65(17)	Florida College System institution presidents; powers and duties	Florida
HB 501 (2017)	Public Records And Meetings/Information	Florida

Law, Statute, & Administrative Code	Title and Link	Federal/Florida
	Technology/Postsecondary Education Institutions	
FLORIDA: RULE CHAPTER: 74-2	Florida Information Resource Security Policies and Standards 74-2.001 Purpose; Definitions; Policy; Applicability; Agency Security Programs; Roles and Responsibilities; Risk Management (Repealed) 74 -2.002 Control of Computers and Information Resources (Repealed) 74 -2.003 Physical Security and Access to Data Processing Facilities (Repealed) 74 -2.004 Logical and Data Access Controls (Repealed) 74 -2.005 Data and System Integrity (Repealed) 74 -2.006 Network Security (Repealed) 74 -2.007 Backup and Disaster Recovery (Repealed) 74 -2.008 Personnel Security and Security Awareness (Repealed) 74 -2.009 Systems Acquisition, Disposal, Auditing, and Reporting (Repealed) 74 -2.010 Standards Adopted (Repealed)	Florida

Table 2. Compliance Regulations: Federal and Florida laws, statutes, and administrative codes pertaining to the Florida College System

7.3 CIS CSC TOP 20



7.4 7.4 CIS CSC TOP 5 CONTROLS WITH EXAMPLES PROVIDED BY SPECIFIC FCS COLLEGES AND MATRIX CROSSWALK.

Ana Roldan

Miami Dade College
Inventory of Authorized and Unauthorized Software

NIST 800-53 Control	**Systems to address controls**
CA-7 [CONTINUOUS MONITORING]	The Institution continuously monitors our security plan, performs periodic security vulnerability scans and follows up with a remediation plan. We are in the process of looking for a SIEM solution.
CM-2 [BASELINE CONFIGURATION]	The institution implemented a standard desktop image based on security best practices. Recently purchase the CIS service to implement device-hardening requirements.
CM-8 [INFORMATION SYSTEM COMPONENT INVENTORY]	Annual inventory is performed at our institution
CM-10 [Software Usage Restrictions]	This institution uses software and associated documentation in accordance with contract agreements and copyright laws
CM-11 [User Installed Software]	Users in this intuition do not have local admin access and therefore cannot install software.
SA-4 [Acquisition Process]	SSAE-16 Review and Security Questionnaire
SC-18 [Mobile Code]	
SC-34 [Non-Modifiable Executable Programs]	
SI-4 [Information System Monitoring]	Firewall and Siem solution
PM-5 [Information System Inventory]	This control does not apply to our institution

Adrian McCray

Hillsborough College
Secure Configuration for Hardware and Software

NIST 800-53 Control	Systems to address controls
CA-7 [CONTINUOUS MONITORING]	
CM-2 [BASELINE CONFIGURATION]	The institution currently maintains a base image used when deploying a system.
CM-3 [CONFIGURATION CHANGE CONTROL]	The institution current maintains various configuration control mechanisms depending on the information system being addressed. For instance: • For Systems Developers and Enterprise Systems, there is a formal Configuration Change control process which requires review and explicit approval before changes are implemented. • For Desktop /Server operating system patch management, the framework is less rigid. Tools Used: • For Development Change Control, proprietary Version Control system is used. • For Operating System Patch management, Microsoft System Center is used.
CM-5 [ACCESS RESTRICTIONS FOR CHANGE]	• Physical Access Controls exist to ensure that only authorized personnel have access to critical systems. • Logical access controls exists to provide that only Tools Used: • Active Directory for logical access controls to systems.
CM-6 [CONFIGURATION SETTINGS]	Tools Used • A Service Catalog was recently introduced to document the implementation and configuration of any new system that is introduced. This Catalog is maintained in a shared document repository accessible by authorized personnel.
CM-7 [LEAST FUNCTIONALITY]	Currently the institution does not have formalized policy on Least Functionality across systems. However, it is generally accepted that most system are single function.
CM-8 [INFORMATION SYSTEM COMPONENT INVENTORY]	The institution leverages Microsoft System Center to perform regular Hardware and Software inventories of computing systems.
CM-9 [CONFIGURATION MANAGEMENT PLAN]	The institution does not have a formalized process to address this control.

CM-11 [USER-INSTALLED SOFTWARE]	The institution does not have a formalized process to address this control.
MA-4 [NONLOCAL MAINTENANCE]	For essential IT systems, non-local maintenance is allowed after successful establishment of a VPN connection to our internal firewall. Authentication is enhanced through a requirement of two factor authentication. Access is controlled through the restriction of communication methods and ports.
RA-5 [VULNERABILITY SCANNING]	Systems on our networks are regularly scanned for vulnerabilities using various tools. These tools include Rapid7 Metasploit and SIEM tools.
SA-4 [ACQUISITION PROCESS]	The institution does not have a formalized process to address this control.
SC-15 [COLLABORATIVE COMPUTING DEVICES]	The institution does not have a formalized process to address this control.
SC-34 [NON-MODIFIABLE EXECUTABLE PROGRAMS]	This control is uniformly applied to purpose-build appliances. There is no tool used to enforce this control.
SI-2 [FLAW REMEDIATION]	Systems on our networks are regularly scanned for vulnerabilities using various tools. These tools include Rapid7 Metasploit and SIEM tools.
SI-4 [INFORMATION SYSTEM MONITORING]	The institution employs centralized event log/syslog collection for correlation and analysis. Additionally, tools are deployed that provide for network analysis and control. Tools Used • ForeScout Network Access Control • System Center Operations Management • Alienvault • FireEye

Mohammad Rahaman

Florida Southwestern State College
Continuous Vulnerability Assessment Remediation

NIST 800-53 Control	**Systems to address controls**
CA-7 [CONTINUOUS MONITORING]	BAE System Monitoring
CM-2 [BASELINE CONFIGURATION]	TraceSecurity
RA-5[Vulnerability Scanning]	
SC-34 [Non-Modifiable Executable Programs]	
SI-4 [Information System Monitoring]	
SI-7 [Software, Firmware, and Information Integrity]	

7.5 INCIDENT HANDLING CHECKLIST (POST EVENT OCCURRENCE)

The implementation of the checklist below aligns with the following incident response guidelines:

- Safeguards should be utilized by the pre-established incident response team, which should consist of:
  - A member of the upper level management team
  - College's Chief Information Officer (CIO)
  - A member of College's Information Security team
  - Member of IT/System Administration team
  - College Attorney
  - Member of Public Relations team
  - Member of Human Resources department
- Organizations must create, provision, and operate a formal incident response capability. Federal law requires Federal agencies to report incidents to the United States Computer Emergency Readiness Team (US-CERT) office within the Department of Homeland Security (DHS).
- Student Aid Internet Gateway (SAIG) Agreement requires that institutions "report actual data breaches, as well as suspected data breaches **on the day** that a data breach is detected or even suspected[5]

	Action	Completed
	Preparation	
1.	Identify and Document Incident Handler Communications Procedures and Facilities	
2.	Acquire and Train Incident Handlers on Use of Incident Analysis Hardware and Software	
3.	Develop, Acquire, Document Incident Analysis Resources	
4.	Implement and Test Incident Mitigation Software	
	Detection and Analysis	
5.	Determine whether an incident has occurred	
5.1	Analyze the precursors and indicators	
5.2	Look for correlating information	
5.3	Perform research (e.g., search engines, knowledge base)	
5.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
6.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
7.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
8.	Acquire, preserve, secure, and document evidence	
9.	Contain the incident	

[5]Federal Student Aid, FSA Cybersecurity Compliance.
https://na01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fifap.ed.gov%2Feannouncements%2FCyber.html&data=02%7C01%7CNBoyer%40polk.edu%7C08515f9d16f847d8c88108d574b637d8%7C6c45d56b3363401abfa8582773cad37e%7C0%7C0%7C636543248355527098&sdata=VsXrZVqjA6i0GxsOZQ3Socip36XxMxcrSNDbSdRVkfI%3D&reserved=0

10.	Eradicate the incident	
10.1	Identify and mitigate all vulnerabilities that were exploited	
10.2	Remove malware, inappropriate materials, and other components	
10.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (5.1, 5.2) to identify all other affected hosts; then contain (8) and eradicate (9) the incident for them	
11.	Recover from the incident	
11.1	Return affected systems to an operationally-ready state	
11.2	Confirm that the affected systems are functioning normally	
11.3	If necessary, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
12.	Create a follow-up report	
13.	Hold a lessons-learned meeting (mandatory for major incidents, optional otherwise)	

Table 1: NIST SP 800-61 R2, Table 3-5, Incident Handling Checklist

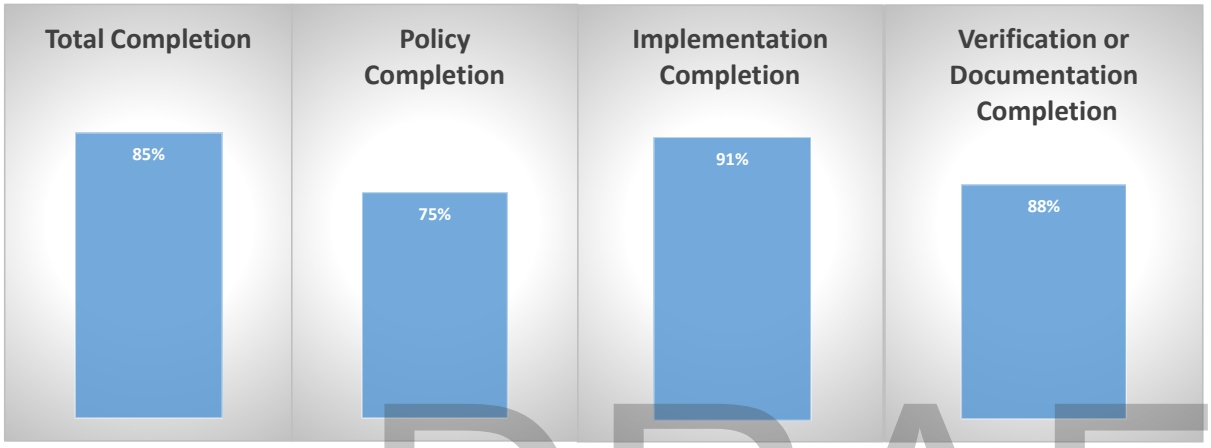
7.6 Florida College System CIO Threat Mitigation Survey: Tools and Techniques*

Respondents

Total Number of Colleges Responding: 19
Broward College Chipola College Daytona State College Florida SouthWestern State College Florida State College at Jacksonville Hillsborough Community College Lake-Sumter State College Miami Dade College Palm Beach State College Pasco-Hernando State College Pensacola State College Polk State College Santa Fe College Seminole State College South Florida State College State College of Florida, Sarasota-Manatee St. Petersburg College Tallahassee Community College Valencia College

* Full survey results are secure content available to those with appropriate approval.

GLBA Safeguards



Policies: 75%
Implementation: 91%
Verification or Documentation: 88%
Total Maturity: 85%

ID	Security Control Detail	NIST Core Framework	Policy Defined	Related Procedure	Total Implementation	Verification (or Documentation where applicable)
1	Institutions must develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue.	Identify	Written Policy, Pending Approval	SCF Information Security Program	Fully Implemented	Verified
2	Institutions must develop, implement and maintain a risk assessment process. Identify and assess the risks to customer information in each relevant area of the company's operations, and evaluate the effectiveness of the current safeguards for controlling	Protect	Written Policy, Pending Approval	Risk Assessment	Fully Implemented	Verified
3	Institutions must design and implement a safeguards program, and regularly monitor and test it to control the risks you identify through regular risk assessments.	Protect	Written Policy, Pending Approval	Vulnerability Management	Fully Implemented	Verified
4	Institutions must designate an employee or set of employees to coordinate and manage the information security program and to coordinate the safeguards.	Detect	Written Policy, Pending Approval	SCF Information Security Program	Fully Implemented	Verified

5	Check references prior to hiring employees who will have access to customer information.	Protect	Written Policy, Pending Approval	Background Screening	Fully Implemented	Verified
6	Ask every new employee to sign an agreement to follow your organization's confidentiality and security standards for handling customer information.	Detect	Written Policy, Pending Approval	Training and Awareness	Fully Implemented	Verified
7	Train employees to take basic steps to maintain the security, confidentiality and integrity of customer information, such as: locking rooms and file cabinets where paper records are kept	Protect	Written Policy, Pending Approval	Training and Awareness Confidentiality Clean Desk-Clear Screen	Fully Implemented	Verified
8	Train employees to take basic steps to maintain the security, confidentiality and integrity of customer information, such as: using password-activated screensavers	Detect	Written Policy, Pending Approval	Training and Awareness Clean Desk-Clear Screen Access Control	Fully Implemented	Verified
9	Train employees to take basic steps to maintain the security, confidentiality and integrity of customer information, such as: using strong passwords (at least eight characters long)	Protect	Written Policy, Pending Approval	Training and Awareness Password	Fully Implemented	Verified
10	Train employees to take basic steps to maintain the security, confidentiality and integrity of customer information, such as: changing passwords periodically, and not posting passwords near employees' computers	Detect	Written Policy, Pending Approval	Training and Awareness Password	Fully Implemented	Verified
11	Train employees to take basic steps to maintain the security, confidentiality and integrity of customer information, such as: encrypting sensitive customer information when it is transmitted electronically over networks or stored online	Protect	Written Policy, Pending Approval	Training and Awareness Data Encryption	Fully Implemented	Verified
12	Train employees to take basic steps to maintain the security, confidentiality and integrity of customer information, such as: referring calls or other requests for customer information to designated individuals who have had safeguards training	Protect	Written Policy, Pending Approval	Training and Awareness	Fully Implemented	Verified
13	Train employees to take basic steps to maintain the security, confidentiality and integrity of customer information, such as: recognizing any fraudulent attempt to obtain customer information and reporting it to appropriate law enforcement agencies.	Protect	Written Policy, Pending Approval	Training and Awareness Incident Response	Fully Implemented	Verified

14	Instruct and regularly remind all employees of your organization's policy and the legal requirement to keep customer information secure and confidential. You may want to provide employees with a detailed description of the kind of customer information you handle (name, address, account number, and any other relevant information) and post reminders about their responsibility for security in areas where such information is stored in file rooms, for example.	Protect	Written Policy, Pending Approval	Training and Awareness Confidentiality Clean Desk-Clear Screen Data Classification	Fully Implemented	Verified, Needs Documentation
15	Limit access to customer information to employees who have a business reason for seeing it. For example, grant access to customer information files to employees who respond to customer inquiries, but only to the extent they need it to do their job.	Protect	Written Policy, Pending Approval	Access Control	Fully Implemented	Verified, Needs Documentation
16	Information Systems include network and software design, and information processing, storage transmission, retrieval, and disposal. Maintain security throughout the life cycle of customer information from data entry to data disposal.	Protect	Written Policy, Pending Approval	Software Development Data Encryption Data Retention and Disposal Network Protection	Fully Implemented	Verified, Needs Documentation
17	Store records in a secure area. Make sure only authorized employees have access to the area. For example: store paper records in a room, cabinet, or other container that is locked when unattended	Protect	Written Policy, Pending Approval	Physical Security	Fully Implemented	Verified, Needs Documentation
18	Ensure that storage areas are protected against destruction or potential damage from physical hazards, like fire or floods;	Protect	Written Policy, Pending Approval	Disaster Recovery	Fully Implemented	Verified, Needs Documentation
19	Store electronic customer information on a secure server that is accessible only with a password or has other security protections and is kept in a physically-secure area;	Protect	Written Policy, Pending Approval	Access Control Backup and Storage Physical Security	Fully Implemented	Verified, Needs Documentation
20	Don't store sensitive customer data on a machine with an Internet connection;	Protect	Written Policy, Pending Approval	Backup and Storage	Fully Implemented	Documented
21	Maintain secure backup media and keep archived data secure, for example, by storing off-line or in a physically-secure area.	Protect	Written Policy, Pending Approval	Backup and Storage Physical Security	Fully Implemented	Documented
22	Provide for secure data transmission (with clear instructions and simple security tools) when you collect or transmit customer information. Specifically: if you collect credit card information or other sensitive financial data, use a Secure Sockets Layer (SSL) or other secure connection so that the information is encrypted in transit	Protect	Written Policy, Pending Approval	Data Encryption	Fully Implemented	Documented

23	If you collect information directly from consumers, make secure transmission automatic. Caution consumers against transmitting sensitive data, like account numbers, via electronic mail	Protect	Written Policy, Pending Approval	Data Encryption Email Usage	Fully Implemented	Documented
24	If you must transmit sensitive data by electronic mail, ensure that such messages are password protected so that only authorized employees have access.	Protect	Written Policy, Pending Approval	Acceptable Use Email Usage	Fully Implemented	Documented
25	Dispose of customer information in a secure manner. For example: - hire or designate a records retention manager to supervise the disposal of records containing nonpublic personal information;	Protect	Written Policy, Pending Approval	Data Retention and Disposal	Fully Implemented	Documented
26	Shred or recycle customer information recorded on paper and store it in a secure area until a recycling service picks it up	Protect	Written Policy, Pending Approval	Data Retention and Disposal	Fully Implemented	Documented
27	Erase all data when disposing of computers, diskettes, magnetic tapes, hard drives or any other electronic media that contain customer information	Protect	Written Policy, Pending Approval	Data Retention and Disposal	Fully Implemented	Documented
28	Effectively destroy the hardware	Protect	Written Policy, Pending Approval	Data Retention and Disposal	Fully Implemented	Documented
29	Promptly dispose of outdated customer information.	Protect	Written Policy, Pending Approval	Data Retention and Disposal	Fully Implemented	Documented
30	Use appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information. For example, supplement each of your customer lists with at least one entry (such as an account number or address) that you control, and monitor use of this entry to detect all unauthorized contacts or charges.	Protect	Written Policy, Pending Approval	Audit Logging	Fully Implemented	Documented
31	Maintain a close inventory of your computers.	Protect	Written Policy, Pending Approval	Language being added to Network Protection	Fully Implemented	Documented
32	Managing System Failures: Effective security management includes the prevention, detection and response to attacks, intrusions or other system failures.	Protect	Written Policy, Pending Approval	Network Scanning Network Protection Firewall Procedure Audit Logging Incident Response	Fully Implemented	Documented
33	Maintain up-to-date and appropriate programs and controls by: following a written contingency plan to address any breaches of your physical, administrative or technical safeguards	Protect	Written Policy, Pending Approval	Incident Response	Fully Implemented	Documented
34	Checking with software vendors regularly to obtain and install patches that resolve software vulnerabilities	Protect	Written Policy, Pending Approval	Patch Management	Partially Implemented	Documented (Partial Implementation)

35	Using anti-virus software that updates automatically	Protect	Written Policy, Pending Approval	Anti-Virus	Partially Implemented	Documented (Partial Implementation)
36	Maintaining up-to-date firewalls, particularly if you use broadband Internet access or allow employees to connect to your network from home or other off-site locations	Protect	Written Policy, Pending Approval	Firewall Procedure Firewall Management	Partially Implemented	Documented (Partial Implementation)
37	Providing central management of security tools for your employees and passing along updates about any security risks or breaches.	Protect	Written Policy, Pending Approval	Training and Awareness	Partially Implemented	Documented (Partial Implementation)
38	Take steps to preserve the security, confidentiality and integrity of customer information in the event of a computer or other technological failure. For example, back up all customer data regularly.	Protect	Written Policy, Pending Approval	Backup and Storage	Partially Implemented	Verified (Partial Implementation)
39	Maintain systems and procedures to ensure that access to nonpublic consumer information is granted only to legitimate and valid users. For example, use tools like passwords combined with personal identifiers to authenticate the identity of customers and others seeking to do business with the financial institution electronically.	Protect	Written Policy, Pending Approval	Access Control Password	Partially Implemented	Verified (Partial Implementation)
40	Notify customers promptly if their nonpublic personal information is subject to loss, damage or unauthorized access.	Protect	Written Policy, Pending Approval	Incident Response	Partially Implemented	Verified (Partial Implementation)

Office of the Provost and Senior Vice President for
Academic Affairs and Student Services
Willis Holcombe Center
111 East Las Olas Boulevard, Fort Lauderdale, FL 33301
Phone 954-201-7067

DATE: July 10, 2018

TO: Council of Presidents

FROM: Council of Student Affairs

SUBJECT: FCS Cybersecurity Ecosystem

This serves as a formal endorsement from the Executive Leadership Team of the Council of Student Affairs for the cybersecurity framework that was developed by the Chief Information Officers (CIO) of the Florida College System.

On June 7, 2018, Dr. Dick Hamann, CIO of Seminole State College of Florida, presented an educational and informative framework that was a culmination of many hours of work with colleagues from the 28 state colleges. The presentation to the Councils of Instructional Affairs and Student Affairs highlighted the importance of implementing a comprehensive cybersecurity framework to strengthen the state colleges' security posture and potentially serve as the rationale that yields additional funding from Tallahassee for this critically important area.

The Council of Student Affairs supports this framework and will support the Chief Information Officers in the implementation of such. Please advise if you require additional information regarding our endorsement.

Respectfully,

Marielena P. DeSanctis, Ph.D.
Chair, Council of Student Affairs
Broward College Provost & Senior Vice-President
for Academic Affairs and Student Services

c: Chair, Council of Information Officers
Council of Student Affairs Executive Leadership Team
Michael Brawer, Executive Director, AFC