PENN STATE UNIVERSITY

123 Corporate Way
Brandywine, Pennsylvania 19343

TO: Jane Doe, CISO

FROM: Ronniesha Tirumalasetty

SUBJECT: Recommendation for Organization, Staffing, and Other Requirements for the Information Security Department for the New PSU Campus

Introduction

This document provided information about the new proposed information security department for the New Penn State campus. The recommendations are given based on the practices at Brandywine university and in accordance with the NIST Guidelines. The document contains the staffing requirements and the organization of the information security team. Policy improvements are also suggested from preexisting PSU policies. The suggestions aim to make the organization more compliant with the general NIST standards. A sample inventory of IT technology is also available for reference.

Organization and Staffing

The duties of the team will be separated to follow the NIST best practices for implementing roles and responsibilities. [1] The team will be managed by the IT Director. The IT Director will serve as the central authority of the organizational units.[2] The supporting roles will include IT technicians troubleshooting and provide technical support for end-users. A Network Systems Specialists will implement NIST protocols to design and implement a secure network infrastructure. The system administrator will be responsible for managing the campuses systems. The Network Security Specialis**t** role is created to incorporate the NIST SP 800-41 guidelines for firewall security. The new campus will need to provide security public and private university networks. The requirements for the role will be to understand how to deploy and maintain secure firewall architecture. According to NIST best practices network access control needs to be monitored. Checks should be made to make sure the firewall software and anti-malware is up to date. The configuration settings for the firewall should also be checked for security. Responsibilities will also include maintaining security logs. System Administrator role is responsible managing access controls for Penn State's user management system. The system will be set up using the least privileged architecture. The role will also be to configure the hardware devices and classroom technology. IT Director role manages the information security team. Additional, responsibilities include coordinating with the with other campus information technology faculty. The director will also manage the department's finances for the new team. The director will also have to make sure the new team maintains compliance with the NIST standards. In addition, to the specialized categories support specialists are also included to assist

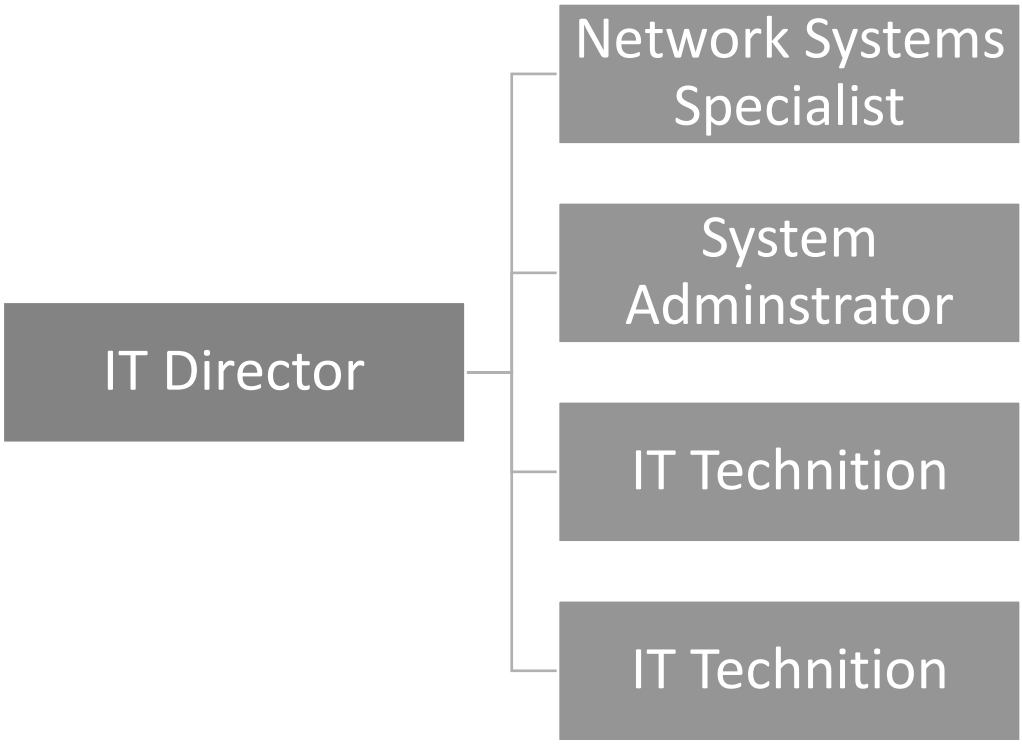
[1] The NIST.SP.800-218 contains information on best practices for preparing the organization.
[2] This structure is based on the NIST 800-50 Diagram.

in day-to-day needs. IT Support Specialists are the responsibilities of IT support specialists who will be providing user support for the end users. They will also provide maintenance for hardware devices. The IT support specialist's role fulfills the NIST incident response requirement.

Organization

The following chart is the proposed organization for the information system.
The organization includes an IT Director, Network Systems Specialist, System Administrator, and IT technicians. Given the size of the campus, it would be beneficial to have limited IT staff but with separate roles. The IT director will be responsible for managing the information security department. The subgroups would include the Network Systems specialist and the System Administrator. The IT technicians will be there to support the existing technologies and assist the end-users.

Chart 1: Proposed Organizational Chart



Staffing

The information in the following table is acquired from the job postings from the industry. The roles are created from the existing Penn State Brandywine IT team. [3] Additional roles, security administrator, were created to improve the account management. The frees up the IT Director's resources as opposed to the existing structure, where there was one IT director, a Network specialist and a support staff. The roles are separated so there can be more focus on access control and system management.

[3] Role descriptions were organized according to the categories from NIST 800-12

Table 1: Proposed Staffing Requirements

Employee Billet	Number Required	Education Required	Industry Certifications Required	Salary Range
Security Administrator	1	B.S Computer Science or Related Degree	Azure Solutions Architect Expert, Oracle Certified Professional, Red Hat Certified Engineer, CompTIA Server+,	80,000 – 120000
Network Security Specialists	1	B.S Computer Science or Related Degree	CompTIA Network+ CompTIA+ Security+ CompTIA PenTest+	75000 – 110000
IT Support Specialist	2	B.S Computer Science or Related Degree	Microsoft Certified IT professional, CompTIA A+	40,000-75,000
IT Director	1	B.S Computer Science or Related Degree	Certified Information Security Manager, Project Management Professional, CISSP	$55,000 - $85,000

Policies Specific to the New Campus

The new information security department will be compliant with the policies of the main campus. Ensuring student information is protected is essential for the organization. However, there are case scenarios where the organization needs to be able to access the data. In accordance with policy AD53 authorized personnel can access the personal information to continue duties. This policy should be followed in accordance with the least privilege principle. Access to the student information should be limited to only those who need it. The policy should be adjusted

so permission must be granted from the security administrator to access the information. In the event student information is required by the university for an external cause a ticket should be submitted, and the request should be logged.

New policies regarding the organization's network security management should be made. This new policy should include instructions for secure practices. This would assist the organization to minimize the risks posed from internal threats. It should also provide guidelines for the network security professional to follow the NIST firewall policy recommendations. Devices should be used as intended firewall security. The NIST[4] guidelines suggest a defense-in-depth approach. This can be achieved through multiple layers of firewalls. Policy should include improved documentation for firewall capabilities.

Table 2: PSU Policies

Policy ID	Policy Title	NIST Compliant	Remarks
AD95	Information Assurance and IT Security	NIST SP 800-53 NIST SP 800-171	
AD53	Privacy Policy	NIST Special Publication 800-53	The university's general privacy guidelines.
AD96	Acceptable Use of University Information Resources		
AD23	Use of Institutional Data		
ADG02	Computer Facility Security	NIST Special Publication 800-53	

Information Security Technology

The following table includes the inventory of the IT resources required for the New Penn State Campus. The figures in the table are acquired from the existing inventory at the Penn State Brandywine campus. The resources include physical classroom equipment, and security devices. The maintenance of the regular classroom equipment should be done through the IT Support Specialists. The following prices are estimates and are subject to change. Desktop computers were included for general classroom use. The calculation for the computer is the estimate for one

[4] Information Sourced from NIST Publication800-41

computer lab with thirty seats. The policy associated with the lab is the general Penn State IT resource usage policy. Podium technology would be utilized by lecturers to present content to a screen. The screens displays are used to display content. The antivirus software can be different depending on the machine. Windows computers automatically come with windows defender. The campus firewall technology can be obtained from companies like CISCO. They are able to set up an enterprise level firewall. Many kinds of devices will be connecting to the network, it is important to secure the connections. JAMX or BigFix is the security technology used by Penn State. This technology should be used to secure devices in the apple ecosystem. SCCM is the technology used for managing Microsoft accounts. The printer device is acquired through the PAW Print system. It is connected throughout the organization and needs to be configured to prevent misuse. The New Campus would require hardware for setting up connections through the ISP. The hardware can include the router, ethernet cables, and range extenders. The exact configuration would need to be determined by the Network Security Specialist.

Table 3: Proposed Information Security Technology

Technology Type	Function	PSU Policy Alignment	Cost	Turnover/Upgrade Rate
Desktop Computers	IST lab computers	AD96	**40,000**[5]	Replaced during hardware failure or gradually phased out.
Podium	Provide access to the screen	AD96	9,000[6]	Replaced during hardware failure.
Classroom Screens	Projection	AD96	31,500[7]	Replaced through warranty
Anti-Virus Software	Protect the hardware and the network.	AD95		n/a
Campus Firewall	Provide Network Security	AD95	6,000[8]	Updated 3-5 Years
JAMF or BigFix	Mac security devices	AD95		n/a
SCCM	Used for managing Microsoft accounts.	AD96	$1,976	Microsoft subscription price.
Wi-Fi	Provide Network	AD96	ISP Payment	n/a

[5] Cost is estimated from a unit price of 730 and 50 machines.
[6] Unit price is 300 and cost is calculated for the estimate of 30 classrooms.
[7] Price based on ViewSonic Pro for 30 classrooms.
[8] Estimated from Cisco Firewall hardware costs.

	Access for the Campus		Plan	
Printer	Hardware to provide printing services.	AD96	PSU Paw Prints System	n/a

Conclusion

The final recommendations for the New PSU Campus include adjusting the suggested policies depending on the budget and resources allocated for the program. The suggested organization improves the security of the IT department because it adds additional roles to secure the organization. The system administrator can ensure the devices are configured with the least privilege and protect the hardware. The network security role ensures the organization follows the NIST protocol for network security. In addition to new roles, policy updates are also suggestions for updated network security policies and user data protection policies.