Project 2: Security Policies

IST 456

Team Algol

Daniel Couillard

Dennis Czaplicki

Timothy Flynn

Stephen Senick

Ryan Snell

Ryan Stramitis

Alan Totten

Table of Contents

Guideline ADG06 2
Policy AD19 4
Policy AD20 6
Policy AD56 8
Policy AD65 10
Guideline ADG02 12
Policy AD22 14
Work Breakdown 17
Works Cited 18

Guideline ADG06

Name of Policy or Guideline

Pennsylvania State University implemented Guideline ADG06 (Appropriate Use of Student Data) in 2009.

Purpose – what does this policy/guideline specify or require?

The purpose of ADG06 focused around the handling of student information on the faculty end according to the 1974 Family Educational Rights and Privacy Act. The purpose of ADG06 is to provide guidelines to members of the Penn State faculty in dealing with legitimate uses of student-generated data such as grades. The first guideline lay out by ADG06 deals with the disclosure of lists of student directory information to parties outside of Penn State University, and how the University would deal with such requests if they feel it would be beneficial to the students. However, the guidelines also specify circumstances where directory information may be shared, such as in the case of job references. ADG06 also states that student information employees can share within the University "for purposes that are beneficial to the student and/or to the University with the understanding that the units receiving those lists provide appropriate privacy and security of those lists according to institutional policy or law". ADG06 goes into further depth in outlining the procedures for dealing with third parties who seek to access the information of Penn State students, specifically when Penn State outsources services or when research organizations gather personally identifiable student information without the students' express consent. In both cases, ADG06 stresses the importance of a contractual agreement between the University and the third party. This contractual agreement between Penn State and the third party must adhere to five key points (six in the case of research organizations) focused on protecting student information and reducing liability.
Finally, ADG06 states that employees of Penn State University can only access the records of students in which they have "legitimate educational interest".

History – why was this policy or guideline developed? Remember that all policies are developed in reaction to something, or to prevent something. Give some thought to what was happening (in technology and in how people used technology) that might have resulted in development of this policy or guideline.

As stated in the preamble of the policy, the University created ADG06 to keep up with the explosion in the use of database technology in storing and transmitting student information electronically. In the past, student records existed in the form of hard copies, which were easy to keep track of. However, as the University went to a more digital storage method, it became obvious to University policymakers that keeping student records secure needed stricter guidelines, especially to keep in line with FERPA. As the University as a whole moved towards an electronic records system, the employees needed to know exactly how information could be viewed and disseminated, especially since electronic data is much easier to share with third parties than data in the past. The University apparently hoped that ADG06 would serve as a good enough guideline for all

employees who are dealing with sensitive student information, as well as protecting the University from any possible mishandling of data.

Revision History – describe how this policy/guideline has been revised since its initial issuance. If there have been many revisions, select 2 major revisions and explain how the policy/guideline was revised and why it was revised.

Pennsylvania State University approved the implementation of ADG06 in October of 2009, and ADG06 became effective on November 4th of the same year. The University has not revised or edited this policy since the University put it into effect. However, it would not be a surprise if the policy underwent changes in the near future. In the six years since the policy's implementation, the digital world has greatly evolved. Students generate increasing amounts of data, and the world is even more interconnected. As information becomes more available, it is necessary that the University continue to stay vigilant.

Policy AD19

Name of Policy or Guideline

Pennsylvania State University implemented Policy AD19 (Use of Penn State Identification Number and Social Security Number) in 2007.

Purpose – what does this policy/guideline specify or require?

The purpose of AD19 is to govern how the Social Security numbers (SSN) and Penn State Identification Numbers (PSU IDs) of students and employees at Penn State are used by the University. AD19 shows the University's commitment to privacy and confidentiality towards the SSNs it stores. According to AD19, PSU IDs are the primary form of identification for Penn State students and faculty. SSNs are only used when required by law. Even then, the University will take action to protect its privacy and confidentiality by storing the SSN in the Central ID Repository as a private data element with limited and encrypted access controls. The Chief Privacy Officer has been given authority to monitor compliance to any federal and state regulations as well as overseeing policy issues within Penn State systems.

History – why was this policy or guideline developed? Remember that all policies are developed in reaction to something, or to prevent something. Give some thought to what was happening (in technology and in how people used technology) that might have resulted in development of this policy or guideline.

This policy was created in response to the rise of identity theft and the need for information security. Prior to this policy, Penn State used SSNs as the primary form of identification. This brought no privacy to an individual's SSN. As the SSN began to become the national identification number from United States citizens, the way Penn State used SSNs had to change. It was not enough to simply change the way Penn State used SSNs however. The way they are stored needed to be changed as well. Information stored on computers needed to be more and more secure as people began to realize that company information could be accessed and stolen in that manner. Policy AD19 changes the primary form of identification from the SSN of an individual to an issued PSU ID. It also explains that SSNs are only to be used when legally required and are to be secured on the Central ID Repository using encryption and access controls.

Revision History – describe how this policy/guideline has been revised since its initial issuance. If there have been many revisions, select 2 major revisions and explain how the policy/guideline was revised and why it was revised.

There have been many revisions to AD19 throughout the years. In April 11, 2007, Penn State revised the policy to show that clinical and patient systems are not exempt from this policy. This is because of security concerns for health information. Penn State wants to make sure that SSNs of its students and employees are private in all ways. This also was probably issued due to HIPAA policies.

Another revision was issued in October 27, 2010. With this revision, Penn State created requirements for how SSNs should be secured and stored within the Central Identification Repository. This was created to ensure the confidentiality, integrity, and availability of the SSNs. With a standard of security and storage to follow, Penn State will also know what is expected of them for their constituents.

Policy AD20

Name of Policy or Guideline

Policy AD20 Computer and Network Security

Purpose – what does this policy/guideline specify or require?

The purpose of the AD20 policy is to provide conditions and requirements for security of the University's Computer and Network Resources. The policy specifies that the information of the University and those within it should be protected against unauthorized access, network attacks, and denial of service attacks. The policy states the responsibilities of those related to the use of computer and network resources including the system's users. Lastly, the policy indicates possible sanctions for those who are in violation of the policy.

History – why was this policy or guideline developed? Remember that all policies are developed in reaction to something, or to prevent something. Give some thought to what was happening (in technology and in how people used technology) that might have resulted in development of this policy or guideline.

The need for a computer and network security policy can be traced back to the emerging computer technology in the early 1980's. In 1981, IBM introduced its first PC, which led to in 1982, Time magazine naming the computer the "Machine of the Year" as opposed to the "Man of the Year." The major need for the policy though can be evident through the ARPANET splitting into the ARPANET (civilian network) and MILNET (military network) in 1983. This split of what is now known as the Internet occurred because of the emergence of the TCP/IP protocols (Computer History). Coincidentally, the policy was created in August of 1983.

Revision History – describe how this policy/guideline has been revised since its initial issuance. If there have been many revisions, select 2 major revisions and explain how the policy/guideline was revised and why it was revised.

Even though the policy was created in 1983 it has had several revisions over the years. In the 1986 the policy was revised to remove the administration of the AD20 from the Director of Computer and Information Systems. In 1992, there was a "substantial rewrite" of the policy possibly due to the rapidly growing Internet and need for an updated proper network and computer security policy. The majority of the revision history happened just over a decade ago in January 2004. Most of the revisions involve clarifying what the University is not responsible for, what the University is allowed to do, and what the University will prohibit. For example, The University will cooperate with all legal requests and the University reserves the right to impose sanctions on those violating the policy, which includes possible expulsion of student(s) and termination of faculty. In addition, servers will not be in campus residence halls unless necessary. This revision prevents students from having easy access to the servers and limits the amount of people who may cross paths with the server room. Previously under the

AD20 policy was a section for copyright and intellectual property but that has now been moved to a whole new policy that solely focuses on copyright infringement.

Policy AD56

Name of Policy or Guideline

Policy AD56 — Use of Group Communication Tools to Communicate University Business to Employees and Students

Purpose – what does this policy/guideline specify or require?

The purpose of Penn State Policy AD56 is to establish standards for communicating with all employees students or subsets therein regarding university business, issues or emergencies. However, the purpose of this policy is not for departmental or college-specific communications; rather, communications that must abide by AD56 are intended for a portion of either the faculty, staff or students at the university. The policy defines group communication tools as "communications sent from University systems, cellular phones, smart phones, or any other device or platforms to a portion of either the faculty, staff or students."

History – why was this policy or guideline developed? Remember that all policies are developed in reaction to something, or to prevent something. Give some thought to what was happening (in technology and in how people used technology) that might have resulted in development of this policy or guideline.

The Pennsylvania State University Policy AD56 was first adopted on September 21, 2000. Unlike some policies that are reactionary, Policy AD56 was developed as a preventative measure against the misuse of communication facilities owned by the university. As electronic communication became more prevalent with regards to mass university communications, standards were developed in order to prevent them from being misused either intentionally or accidentally. The main use case that this policy is to be applied to is mass notifications in the event of an emergency. However, while that is the primary use case, other types of notifications must also abide by the policy.

The policy may also be applied in contexts outside of emergency management and response. For example, the use of Policy AD56 may also be applied to research initiatives. In order to obtain participants for research studies, recruitment must be performed. This recruitment may be done through traditional methods such as print advertisements or through digital media. However, if electronic communications are used that match the definition of "group communication tools" as defined in the policy, such research recruitment efforts must abide by the policy as to prohibit unsolicited emails to Penn State University recipients.

Revision History – describe how this policy/guideline has been revised since its initial issuance. If there have been many revisions, select 2 major revisions and explain how the policy/guideline was revised and why it was revised.

Since the policy's adoption in 2000, it has been revised three times. On January 21, 2003, an editorial change was made to change "Vice President for Administration" to

“Vice President for University Relations.” This change was most likely due to a title change. On March 30, 2010, the definition of group communication tools was modified to reflect changing technology. Finally, the most recent change to the policy occurred on June 9, 2014, in which there were various edits made to reflect current operations of communications facilities used by the university. In addition, a policy steward and further information references were added in order to increase the sustainability of the policy.

Policy AD65

Name of Policy or Guideline

AD65 Electronic Security and Access Systems

Purpose – what does this policy/guideline specify or require?

This policy entails a few different aspects, all of which regard electronic and access systems as well as electronic security for those systems. First off, this policy is intended to promote both practices and protocols that that overlook the assessment of physical security needs. Also, these practices and protocols look at other aspects of electronic security systems within the Pennsylvania State University including: the design, specification, installation, testing, acceptance, maintenance, and operation. It should also be noted that the systems that follow under this policy are in facilities that are owned, leased, or under control of the Pennsylvania State University. However, Hershey Medical Center, the College of Medicine, and the Pennsylvania College of Technology are excluded from this.

It is written that it is a policy of the University to keep an open access environment for students, faculty, staff and so forth. With this policy however comes a need for an environment that is kept both safe and secure by the University and this done by developing standards for electronic security and access control. Additionally, any new electronic or access systems that are implemented in any Pennsylvania State University facility must be integrated with the central access control and be compatible with the University ID card.

History – why was this policy or guideline developed? Remember that all policies are developed in reaction to something, or to prevent something. Give some thought to what was happening (in technology and in how people used technology) that might have resulted in development of this policy or guideline.

This policy was approved on March 29, 2010 and it was published and deemed active the very next day. The main reason that this program was designed was to “implement technically and operationally integrated security systems, enterprise-wide.” This basically means that the University wanted to have a universal security system which would encompass all electronic systems and access systems. By doing this, you are able to keep everything uniform in nature and can have security standards and protocols that are the same for every system rather than having different standards for different electronic systems. This policy was also developed to ensure that the electronic systems and access systems on the campuses and in the various facilities are secure and can be used by students and faculty safely and without worry. To do this, systems must comply with the standards set and continually update their systems to ensure that they are all secure and safe to use. It is important for the systems and security protocols to be continually updated because of new threats evolving every day. An example of this would be that one day your security may work against a certain type

of malware and the next it may not as the malware has evolved and is able to get around your security measures.

Revision History – describe how this policy/guideline has been revised since its initial issuance. If there have been many revisions, select 2 major revisions and explain how the policy/guideline was revised and why it was revised.

There were two changes to this policy. The first change occurred on March 30, 2010. This was considered a major rewrite of the entire policy. It was done in order to "reflect updates and improvements to the policies, practices, protocols and best practices as they relate to electronic security and access systems at Penn State University facilities." In other words, the University wanted to update everything in regard to security of electronic systems to ensure that everything was update with current threats and that they best protection available is being provided. This change happened once and it will most likely happen again due to the rapidly changing world of electronic security as hackers find new ways to exploit electronic systems every day. This policy was most likely revised as they faced a new threat or potential exploit to their system that was not previously in there or did not have any protocols in place in the event that the threat came up. Also, the policy was renamed as an administrative policy because of the information it contained which deemed it an administrative matter. On January 29, 2014, there was a slight editing change done to the policy. It was updated to show the change of the Risk Management and Privacy Office as separate offices. There was also information added to clear up any confusion or answer any questions about the change to the policy.

Guideline ADG02

Name of Policy or Guideline

ADG02 - Computer Security (Formerly Computer Facility Security)

Purpose – what does this policy/guideline specify or require?

The purpose of this guideline is to establish a set of criteria for access, controls, and security for computers and networks maintained by the University. It defines the responsibilities of Security Operations and Services Director which include removing any hardware that poses a security risk to University networks, revoking access of any accounts found to be partaking in suspicious or malicious activity, and investigating any malicious activity on Penn State networks quickly and fully. It also references ADG01 and states that all accounts must be for individuals with group accounts only being allowed with explicit permission. This ensures that any security violations can be traced to an individual user. This guideline also requires the existence of the Penn State Computer Security Incident Response Team, which is tasked with investigating any computer security breaches.

History – why was this policy or guideline developed? Remember that all policies are developed in reaction to something, or to prevent something. Give some thought to what was happening (in technology and in how people used technology) that might have resulted in development of this policy or guideline.

This guideline was first created in 1997 and was titled “Computer Facility Security”. At this time, the dot-com boom was just kicking off and the internet was becoming increasingly widespread. Also, personal computers and computer labs were becoming commonplace. Within Penn State, computers were shifting from the tools of programmers and researchers to things that all students relied on. Due to this increased traffic in microcomputing labs, security guidelines needed to be developed to govern those facilities. ADG02 applied initially to “computing facilities” and was eventually generalized to “computer security” as computer began to permeate all parts of the University, not just designated areas.

Revision History – describe how this policy/guideline has been revised since its initial issuance. If there have been many revisions, select 2 major revisions and explain how the policy/guideline was revised and why it was revised.

In August of 2005, the guideline was revised to specify that every Penn State network must adhere to the same security guidelines. Previously it had only applied to “Trusted Networks”. This revision was aimed at making all networks more secure and ultimately protecting the information of students and faculty.

In April of 2014, the guideline was revised to reflect the current responsibilities of the Security Operations and Services Director. Since the last revision in 2005, the number

of computers and networks within the University has increased dramatically and this revision ensures that policies reflect a more current security landscape.

Policy AD22

Name of Policy or Guideline

Policy AD22: Health Insurance Portability and Accountability Act

Purpose – what does this policy/guideline specify or require?

To describe the University's responsibilities under the Privacy Rule and related regulations issued under the Health Insurance Portability and Accountability Act (HIPAA) of 1996.
This policy covers all the information that may be stored in the following units on campus:

- University Health Service
- Financial office for Student affairs and the College of Liberal Arts
- Psychological clinic (Dept. of Psychology)
- Penn State Health Plans
- Records Center
- Department of document Services
- Auxiliary and Business services
- Waste Management program (OPP)
- Penn State Privacy Office
- Internal Auditing
- Counseling and Psychological services (CAPS)

In addition to the areas listed above, the policy goes into detail to describe what specific information must be protected, which they refer to as "Protected health information". They define Protected health information as individually identifiable health information that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual.
Following these definitions, the policy goes into detail about how any stored PHI may be used and in any usage, how it should be stored, transmitted and disposed of after its usage. The various usages are listed below:

- Clinical Treatment
- Billing
- Standard Electronic Transactions
- Quality Improvement Activities
- Minimum Necessary Disclosure
- Security of PHI
- Develop Access Control of PHI
- Notice of Privacy Practices
- Use of Support Services from Outside Vendors
- Access to PHI by other University Units and Employees
- Disposal of Paper and Electronic Records and Media Containing PHI

· Research

PHI may also be used in emergency situations as long as certain criteria are met before it is used. These situations are described below:

· Authorization
· As Required by Law
· To avert a Serious Threat to Health and Safety
· Individuals Involved in a Patient's Care
· Public Health Risks
· Health Oversight Activities
· Military and Veterans
· Workers' Compensation
· Lawsuits and Disputes
· Law Enforcement
· National Security and Intelligence Activities
· Protective Services of the President of the United States and Others
· Inmates
· Coroners, Medical Examiners and Funeral Directors
· Accounting for Disclosures

History – why was this policy or guideline developed? Remember that all policies are developed in reaction to something, or to prevent something. Give some thought to what was happening (in technology and in how people used technology) that might have resulted in development of this policy or guideline.

This policy was created on April 14, 2003. Due to the rapid expansion of electronically data, it comes as no surprise that Penn State was required to take these steps early on. Since many of the policies at the time were probably weak in terms of file transfer and storage etiquette, policy makers had to move fast to stem the potential leak of employee and student information.

Revision History – describe how this policy/guideline has been revised since its initial issuance. If there have been many revisions, select 2 major revisions and explain how the policy/guideline was revised and why it was revised.

It does seem evident that Penn State may have been a bit slow to enact some of these information protection policies, however. By examining the list of revisions located at the bottom of this policy, anyone can see that the revisions were simply address changes to describe where the privacy office moved to on campus. Since the document has stayed mostly intact for the majority of its life and the policy itself seems to be very mature and covers many different situations that might have been hard to think of at the time of its conception, it might be deduced that the bulk of its content was derived from some other existing document. If this is the case, Penn State would simply have been following suit of some other establishment that had already employed similar policies.

The most recent change occurred in January of 2013 and consisted of the addition of CAPS services to the list of covered components required to meet specific standards. Also, the policy was renamed as an administrative policy because of the information it contained which deemed it an administrative matter. On January 29, 2014, there was a slight editing change done to the policy. It was updated to show the change of the Risk Management and Privacy Office as separate offices. There was also information added to clear up any confusion or answer any questions about the change to the policy.

Work Breakdown

Name	Policy or Guideline
Dan Couillard	AD22
Alan Totten	AD20
Dennis Czaplicki	AD65
Tim Flynn	ADG02
Ryan Stramitis	AD19
Stephen Senick	ADG06
Ryan Snell	AD56

Works Cited

"Computer History Museum | Timeline of Computer History : Year 1983 Entries." *Computer History Museum* | *Timeline of Computer History : Year 1983 Entries*. Computer History Museum, n.d. Web. 21 Mar. 2015. <http://www.computerhistory.org/timeline/?year=1983>.