Developing an Information Security Program (ISP) for the Town of Nantucket

Nantucket Project Center

An Interactive Qualifying Project Report submitted to the Faculty of

WORCESTER POLYTECHNIC INSTITUTE

In partial fulfillment of the requirements for the Degree of Bachelor of Science

Submitted by

Chris Carrigan

Josh Janssen

David McGinnis

Sponsoring Agency

Information Technology Department of the Town of Nantucket

Advisor

Dominic Golding

Liaison

Linda Rhodes

December 9, 2010

Abstract

This Interactive Qualifying Project report to the Information Technology Department of the Town of Nantucket, discusses the importance of developing an Information Security Program (ISP) for town departments. The report details the history of information security risks, actions that were taken in response, and a thorough analysis of information security procedures. Our group utilized electronic surveys and interviews to gather feedback regarding the opinions of town employees on the security of information within the town departments and what specifics must be included within the ISP. The final product for this project provides a framework for a comprehensive security policy, and our findings create a detailed guide that will aid with the finalization and implementation of the ISP.

Acknowledgements

This report could not have been completely by just the three students; it was a combination of Worcester Polytechnic Institute and the Information Technology Department of the Town of Nantucket. We would like to give thanks to our advisor, Professor Dominic Golding for his assistance with our proposal and his continued help and guidance throughout the past sixteen weeks of our project. We would like to thank our sponsor liaison, Linda Rhodes and the other two members of the IT Department, Molly Sprouse and Patrick McGloin for their continuous feedback and aid throughout the project. We would like to thank all of the departments that completed our surveys and then who we later interviewed to gain more specific details and opinions. If we did not receive help from all of these people, then our project would be non-existent. Thanks again for all the time you spent assisting us.

Executive Summary

This project was sponsored by the Information Technology Department of the Town of Nantucket and its purpose was to improve the security of personally identifiable information that is used, stored, and disposed of by various town departments. Nantucket is a small island which contains roughly ten-thousand year-round residents. Even though Nantucket is smaller than many other towns in Massachusetts, it has numerous municipal departments and offices in various locations. The IT department services and maintains the network for over twenty of these departments. With no formal policies in place, the IT department recognizes the necessity for information security and more specifically the creation and implementation of an Information Security Program, a written management system designed to safeguard sensitive information such as personal information.

The goal of this project was to assist the IT department of the town of Nantucket in the development of a comprehensive ISP. The project team accomplished its goal by completing three objectives. Through surveys and interviews, we identified and compared the current state of information security within the Nantucket town offices to the best practices utilized elsewhere. This allowed us to define what is meant by Personally Identifiable Information (PII) in the Nantucket context and map out the flow of information, from creation to deletion, among Nantucket's different departments. Lastly, we developed draft information security policies and procedures that the Town of Nantucket may implement in future.

Background

Every year, corporations and large government agencies research and develop ways to improve their Information Security Programs (ISP). Even with safeguards in

place, there are numerous breaches ranging from virus attacks to financial fraud to human error. Given the changing nature of the threats, information security policies and procedures must be constantly monitored and revised to remain effective.

On the federal level, agencies such as the National Institute of Standards and Technology (NIST) issue regulations and standards, such as the Federal Information Processing Standards (FIPS) that are mandatory for all federal government agencies.

Legislation is also passed on the state level, such as 201 CMR 17.00, issued by the Massachusetts Office of Consumer Affairs and Business Regulation. This particular piece of legislation requires all entities that possess and handle personal information to create an Information Security Program, although this does not yet apply to municipal governments in the state.

ISPs vary widely depending on the size, scope and purpose of the organization and there is no standard form. Generally, however, an ISP consists of multiple components. Following an initial risk management exercise to identify the potential risks and sensitive information various policies are developed that address all forms of security issues, from proper disposal methods to the security of physical assets.

Methodology

The project team accomplished its goal by completing three objectives. We identified and compared the current state of information security within the Nantucket town offices to the best practices used by other towns and universities. First, background research was conducted on the best and most current security policies used by towns, corporations, and schools. Based on feedback from the surveys and interviews with town officials, our group formed conclusions about the state of Nantucket's level of security

and developed an operational definition of personally identifiable information (PII) to directly apply to the Town of Nantucket. Finally, in conjunction with the IT Department our group drafted individual policies that make up an ISP. These drafted policies will serve as a foundation for the IT Department to produce finalized policies that they can implement among the town offices.

Findings

Our group received thirty of the thirty-six surveys distributed to key personnel in each department. From these surveys and seven follow-up interviews, our group assessed each town department's level of information security and identified improvements that could be made. Based on the completed surveys our group received, eighty-nine percent of the departments handle PII.

Of the departments that handle PII, only three of them track employee access of PII. In these cases, each employee is tracked using the employee's username, timestamp of access, and any editions. Other feedback from the surveys revealed that approximately sixty-three percent of the departments have virus protection systems in place and roughly seventy percent have web access restrictions. Firewalls were utilized by fifty-six percent of the departments, most of these being departments that handle the largest volume of PII. These departments are: Town Administration, Council on Aging, Department of Public Works (DPW), Finance Department, IT Department, Health Department, Our Island Home (OIH), Park & Recreation, and Wannacomet Water Company.

In terms of the physical security of PII, fifty-five percent of the departments surveyed dispose of hard copy files within their offices, all by shredding and then discarding. The same percentage have town issued laptops that are for specific use

within the department, however, none of these departments store PII on any of these laptops. This is fortunate because laptops are considered mobile devices and are a high risk for possible theft. Only one of the departments stores PII on external devices which are exclusively used within the office and only for transferring of data from one computer to another. Fifty-six percent of the departments store hard copies in locked filing cabinets and several store filing cabinets within vaults. Finally only two of the departments, the Council on Aging and OIH, conduct peer incident reporting and have established security policies. Of all the departments that were surveyed and interviewed, OIH had the best security practices in place.

Conclusions and Recommendations

Based on the survey results and feedback from our interviews, we conclude that the frequency of changing a password for user login to the server was too high. Employees had to change their passwords every thirty days and most agreed that every ninety days was much more reasonable. It is our recommendation that the time between passwords be no less than ninety days.

Based on the surveys and interviews it was revealed that several department servers were located in common areas very accessible to employees and/or to the public. Although the server's had locked doors on them, it is still a security risk to not have the servers in a locked room. It is our recommendation to move the servers in question into locked rooms where only administrators and approved employees have access.

Based on the survey results and feedback from our interviews, specifically with Finance, Historical District Commission (HDC) and OIH, we conclude that there is a lack of information security training for current and new employees within town departments.

We recommend that the Town develop a common training program to be administered to current and new employees.

Many respondents in several departments complained that the web access was too restrictive and hampered productivity. A new program for web access, Surf Control, is currently being tested by the IT Department. We recommend that this or similar software be used to give each town department customized web access.

We recommend that the IT Department develop an application that would allow town departments to submit helpdesk and equipment requests to the IT Department online. This application would help organize and prioritize requests and increase efficiencies by streamlining the process for all parties.

Finally, based on the risk assessment that we have conducted through interviews and surveys, as well as the lessons learned from best practices elsewhere, we have drafted a comprehensive ISP that is tailored to the nature of the security risks and the needs of the different town departments (see Appendix C). Within Appendix C are the numerous information security policies that our group, drafted in cooperation with the IT Department. These drafted policies will be the foundation for the future Master ISP that the IT Department will implement in the next year. We recommend that the IT department refine these policies and begin implementing them as soon as possible in order to protect the security of Personally Identifiable Information in the various town departments. Our hope, upon completing this project and policies, is that the Town of Nantucket's ISP will serve as an example for other towns.

Authorship

This interdisciplinary qualifying project was completed with equal contribution of all three members of the Information Technology team: Chris Carrigan, Josh Janssen, and David McGinnis. All sections were created as a team and editing was done equally by all team members.

Table of Contents

List of Figures

List of Tables

I. Introduction

Advances in technology have made storage, usage, and the flow of information convenient, but risky. There are numerous types of security breaches that threaten many types of sensitive information from personal banking and medical files to state secrets. Breaches such as hackers stealing personal information to gain access to bank accounts or disgruntled employees stealing government or trade secrets and selling them to the highest bidder occur on a daily basis. Without a comprehensive Information Security Program (ISP), sensitive information is vulnerable. ISPs have proven to be effective, but unfortunately, many smaller organizations, such as municipal government offices in Massachusetts, do not implement them because of lack of staff, resources or both. Nevertheless, there is a growing concern about security. The town of Nantucket has some policies currently in place to secure sensitive information, the most common being Personally Identifiable Information (PII), but no comprehensive ISP.

With no formal, comprehensive policy in place, Nantucket has only an ad hoc arrangement of procedures to govern how information is accessed, stored, used and disposed. It was therefore in the best interest of the Town of Nantucket that the IT Department to develop an ISP to bring the town's security to the level of best practice in corporations and larger organizations, such as universities. The IT department of Nantucket had started the daunting task of developing a comprehensive ISP, but they were a long way from being finished. Among other things, the IT Department needed to know how information was used, stored, and accessed in the various town departments before they could develop appropriate policies and procedures to ensure greater information security.

The goal of this project was to assist the IT department of the town of Nantucket in the development of a comprehensive ISP. The project team accomplished its goal by completing three objectives. We identified and compared the current state of information security within the Nantucket town offices to the best practices utilized in industry. This led to defining what is meant by Personally Identifiable Information (PII) in the Nantucket context and mapping out the flow of information, from creation to deletion, among Nantucket's different departments through the use of surveys and interviews. Lastly, we developed draft information security policies and procedures that the Town of Nantucket may implement in future. In the proposal that follows, we discuss the issue of information security and why ISPs are important in the literature review. We will also discuss and map out how we plan to accomplish the project goals and objectives in the methods section below.

II. Literature Review

Although organizations have made significant advances within the field of information security, the field itself is constantly evolving and the need to adapt becomes more critical with the increasing number and sophistication of security threats. Organizations implement Information Security Programs (ISPs) with the hope that their initiative to stay ahead of threats is rewarded with no incidents or breaches of security. In this review of the literature, we define what we mean by an ISP and examine the key components that constitute best practices based on a review of ISPs developed and implemented in universities, government agencies, and non-profit organizations. We also review the history and development of ISPs to show how researching the changing nature of the threats and legislation has influenced the field. We review the current legislation at the local, state, and federal level to highlight current and likely future obligations that may be required of local government.

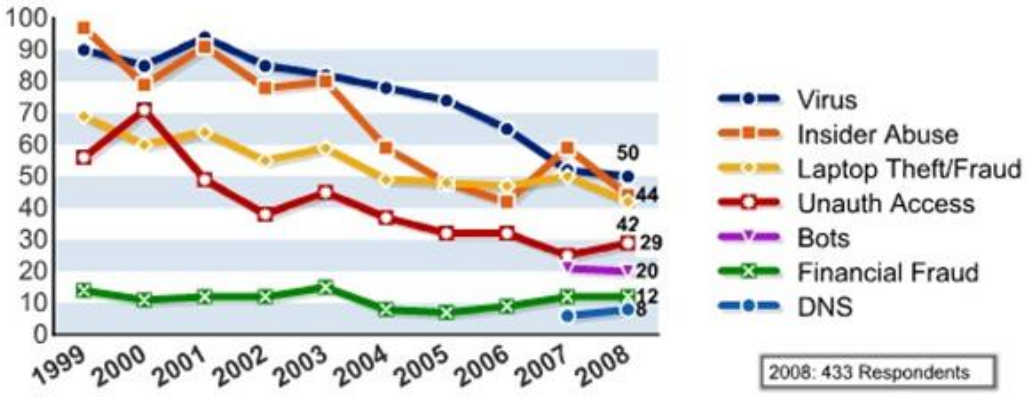
2.1 The Big Picture

We live in a world based on technology and with this dependency a new area of crime and risk develops. With the frequency that personal information is used and stored in a virtual setting, there is a growing concern about the safeguarding information. Ever since the cold war ended, the threat and fear of cyber-terrorism has been a major concern for governments around the world. To a greater or lesser degree, all governments, whether they are totalitarian or democratic, employ large numbers of "personnel for monitoring, analyzing and countering any perceived risks and threats of the global network society" (Eriksson, & Giacomello, 2006). Terrorist plots are but one small part

of the landscape of threats that range from intellectual property theft to scams involving personal information, and they necessarily involve all levels of government.

The Computer Security Institute (CSI), conducts an annual survey of corporations and government agencies that identifies the most common and costly types of security breaches. Figure 1 shows there are many types of threats to information security ranging from the most common, malicious software attacks or viruses, to the more expensive but not as frequent financial fraud (Richardson, 2008). Figure 1 also shows that the proportion of survey respondents experiencing each type of breach has declined over the last 10 years, except with regard to bots, financial fraud, and Domain Name Servers (DNS). It is reasonable to assume that this decline results from the development and implementation of improved security measures. Each of these types of abuse may require different types of security measures, and collectively they indicate the need for comprehensive Information Security Programs (ISPs).

Figure 1: Percentages of Key Types of Security Breaches (Richardson, 2008)



With all of the time and resources that go into the production and implementation of a comprehensive ISP, is it even worth it? The short answer is yes. The Computer Security

Institute (CSI) found in their survey that on average, the respondents from various companies and entities reported average annual losses of $300,000 from all of the combined types of security breaches (Richardson, 2008). Does all of this time and effort make a difference in the end? The CSI, directed by Robert Richardson, conducted an in-depth Computer Crime and Security Survey of 522 computer security practitioners in various corporations, government agencies, financial institutions, medical institutions and universities. The study found a significant drop (Figure 1) in the number of breaches in security (Richardson, 2008). This survey shows that efforts made by different institutions across the U.S are extremely effective in the protection of personal information.

There is a wide variety of threats to information security. A need for a comprehensive Information Security Program (ISP) is continually growing as the types of security breaches continue to evolve. Of all the corporations and agencies questioned by the CSI survey, 68% reported having formal ISPs and 18% reported that they were in the development stages of one (Richardson, 2008). According to Figure 1, the number of incidences of security breaches has shown an overall downward trend and the common factor is the presence of an ISP. This clearly shows that security policies and procedures can have a substantial positive impact, but given the constantly changing nature of the threats such policies and procedures need to be constantly revised and updated.

The most common breach of security faced by corporations and government agencies is the computer virus. Computer viruses come in all shapes and sizes; from an email "phishing" for private account information to viruses that spread rapidly and infect and crash systems on a large scale. A virus is a self-replicating program designed to infect and cripple work stations and networks (The Economist, 2005). One of the first

successful virus attacks, and also one of the largest, was the "Love Bug" worm of 2000. As soon as someone opened the attached 'love letter' from an anonymous secret admirer, the viruses called a worm infected the computer, reproduced itself, then hijacked email addresses from the computer and sent itself out to re-infect. The worm also destroyed data files on the infected computers and stole passwords, causing an estimated $10 billion in damages worldwide (Techweb, 2006).

Viruses are designed to circumvent extant security measures and so they are constantly changing. A person with basic knowledge of computer science and coding can create a virus, which is why they are the most common threat faced by corporations and other organizations. Viruses cost an average of $40,000 per organization each year in terms of time, resources and damaged assets. This is a relatively small amount for a large corporation, but a substantial collective cost to society (Richardson, 2008). Thus, information security measures must be continually upgraded to track and meet the evolving threats. As a result a substantial sector of the software industry is responsible for developing and maintaining virus protection packages.

The second most prevalent threat to information security is insider abuse. This breach of security ranges broadly in terms of severity from something as small as an employee telling a fellow co-worker their password to an employee accessing highly confidential information such as company trade secrets or financial information of customers and selling this information to the highest bidder.

The most expensive breach of security is financial fraud, although this occurs less commonly than most of the other types of breaches. Financial fraud cost an average of almost $500,000 per organization in 2008. Such breaches usually occur deliberately and

at the executive level (wisegeek.com, 2010). One of the biggest and very famous examples of financial fraud is the fall of Enron, a former leader in the energy business. The unauthorized and unethical actions of the few greedy top level executives caused a former multibillion dollar company to fall and file for bankruptcy (Mclean, & Elkind. 2003).

Lastly, companies and corporations have to deal with unintentional breaches of security. Sometimes unintentional breaches are due to natural disasters such floods or earthquakes. More often, though, human error is the cause and often the result of carelessness of staff in possession of sensitive information. For example, in September of 2010, an officer of Gwent Police in the UK accidently sent 10,000 criminal records to a journalist. These records have both personal and sensitive information. Even though there were new security measures implemented earlier that year, lack of training and human error was the cause of a major security breach (Cowan, 2010). The repercussions of such a breach of security are great. A study in 2003 showed that 20% of threat sources came from accidental error (Bryes, & Lowe, 2004).

Large corporations have the most complete ISPs to protect all of their client information and trade secrets from the various breaches of security that they face. Corporations create entire departments whose roles and responsibilities are solely related to information security, and it is these departments that create and maintain the ISPs. Corporations spend these resources to develop ISPs because they make the assessment that avoiding breaches in security proactively is far cheaper than the direct and indirect costs incurred if breaches occur. Consequently, few corporations publish the details of their ISPs or are willing to discuss them publicly. Needless to say, a hacker's job

becomes infinitely easier if they know the template of the ISP they are trying to breach. This lack of information about corporate ISPs forces us to center our attention on the examples of ISPs put in place by universities and government agencies which are more readily available.

Information security is not only a concern for large corporations and government agencies. Everyone has some sort of information that they want kept secure. Whether it is a Social Security number or a bank account number, personal information is very common. Threats to personal information are just as common and it takes awareness and constant vigilance to protect personal information. The most common threat to personal information is identity theft. One example of this type of crime is that of Stacy Sullivan, a writer for *The New York Times*. An individual stole her Social Security number and set up a phone account with her credit. Even after a frustrating four years of providing copious amounts of evidence proving her innocence, and cleared of responsibility for the debts. It was too late; the damage done by others was still reflected poorly on her credit rating (Sovern, 2004). In her article, "How I Lost My Good Name", Sullivan states:

> "The most maddening aspect of all this is that it could have been prevented had the phone companies simply checked the identity of the person who established phone service in my name. Is it too much to ask that companies that issue credit cards sell merchandise or provide services take simple precautions to identify their customers?" (Sullivan, 2000).

Cases similar to this are very common. On average, the cost to the victim of identity theft is $496 in unrecovered losses and legal fees. This number was a significant

decrease from previous years, however, the number of incidences increased by 22% to 9.9 Million (Associated Press, 2009). Even though there was a drop in the average cost, associated with early detection and prevention by the victims, identity theft and cybercrime in general is still increasing. Thus, there is a growing need for information security policies and programs to ordinary citizens protect their personal information. Anything containing a person's name coupled with a social security number, driver's license number or credit card number (201 CMR 17.00: M.G.L. c. 93H, 2010) is more than enough information for a hacker to do severe damage.

A recent study conducted by Javelin Strategy and Research shows the increase of incidences where private information was compromised. There were approximately 11.1 million identity fraud victims in 2009, a 12 percent increase from the previous year and this increasing trend is only continuing in 2010. Attackers were able to steal $54 billion in 2009 from these victims (Klein, 2010), which is a staggering number and shows how information security is a growing concern for everyone who has anything worth protecting.

2.2 Government Legislation

To combat the vast variety of threats to information security, various pieces of legislation have been developed over the years to encourage greater security in the collection, storage, and handling of sensitive information, whether it's physical or digital, and it is likely that future legislation will mandate such policies for state and local government. In the next section, we review the current legislative requirements in Massachusetts and explain how the legislation has changed over the years

2.2.1 History and Background

With the enormous increase in the amount of digital data stored and accessed each year, legislators have become concerned about security and passed state and federal legislation designed to protect privacy. As the volume of digital information has increased and the nature of the threats have changed, so too has the legislation, policies, and programs intended to protect privacy evolved.

The first act that addressed information security was the Privacy Act of 1974. It prohibits unauthorized disclosures of the records it protects. It gives each individual the right to review their own records to find out if records have been disclosed and to change any personal information in any document (Federal Trade Commission, 2007). This is geared more towards the individual rather than the government or corporations.

In 1987, Ronald Regan, the 40th president of the United States, signed the Computer Security Act. "In 1987, the U.S. Congress, led by Rep. Jack Brooks, enacted a law reaffirming that the National Institute for Standards and Technology (NIST), a division of the Department of Commerce, was responsible for the security of unclassified, non-military government computer systems" (Electronic Privacy Information Center, 2010). This was one of the first committees set up to address the problem of cyber security.

In 1988, the Computer Matching and Privacy Protection Act was implemented as a revision to the 1974 act and essentially addressed the issue of expanding computer use. At this time computers were becoming more widespread and information was starting to flow more quickly and with greater ease, so this revision included components of the last act, but included a new section on computer use. Furthermore,

the act allowed federal agencies to share information for various purposes without the need for permission. The act was seen as including integrity and fairness, but lacking in privacy (Privacilla, 2001).

The earliest attempts to enhance information security within the federal government occurred when the General Accounting Office started to limit the number of federal employees who could access computers. Limiting the number of people with access to information was intended to decrease the likelihood of a breach. In 1983, the Federal Bureau of Investigation took a more offensive approach and raided homes and confiscating Telnet passwords, computers, one laptop, and a modem from people suspected of accessing or leaking sensitive information. In the same year Floyd Clarke, Deputy Assistant FBI Director, told a subcommittee of the House that a computer can be utilized much like "a gun, a knife, or a forger's pen," and urged Congress to pass new legislation. This foreshadows future problems and helps to show the emerging concern about internet security. Approximately a decade later Michelle Van Cleave, the White House Assistant Director for National Security Affairs, categorized hacking as "a serious strategic threat to national security," (washingtonpost.com, 2003) this shows how concern has developed from just a threat in 1983 to a threat to national security in 1991.

The Health insurance Portability and Accountability Act (HIPAA) was introduced in 1996 and was the first development in the healthcare industry that addressed information security. It forced the Department of Health and Human Services to formulate national standards for electronic health care transactions (US Department of Health and Human Services, 2010).

In 1998, President Clinton appoints John Koskinen, former Deputy Budget Director, to chair his Year 2000 Conversion Council. One of the duties of this council is to set a template for an executive branch that will be formed in the future to address cyber security threats. Later in the same year President Clinton required the government to work closely with businesses to protect the nation's vital information systems as nearly 90 percent are privately owned and operated by these businesses. The President also appointed Richard Clarke as the National Coordinator for Security, Infrastructure Protection, and Counter-terrorism and requests that a national cyberspace protection plan be implemented by 2000. When this strategy was released in January 2000 it received good reviews from the industry even though the government developed the plan behind closed doors and with little industry input.

In October 2001, George W. Bush created the President's Critical Infrastructure Protection Board with the responsibility for developing a national cyber security plan. The board began gaining advice from private contacts and held town-hall meetings to receive input from a variety of sources to form its cyber security plan. In September 2002 the cyber security plan was released. It had cut back on the controversial provisions; one of these requiring high-speed internet service providers to sell firewall products with their internet services. They also omitted an industry-fed cyber security fund and a section on denying the use of emerging wireless networks until they are approved. This is criticized as not being firm enough so the White House started to work on a subsequent plan. While the second plan was being drafted, President Bush signed the "Cyber security Research & Development Act," in November 2002, which required $900 million to be spent over five years for security research and education. He also

signed legislation that created the Department of Homeland Security and increased the legal penalties for computer crimes. This department absorbed five pre-existing cyber security offices and programs and became the leading department for cyber security. The second draft of the cyber security plan included practical tips for businesses to keep their networks safe, as well as home internet users. It also requests government contingency plans in case a major section of the Internet is shut down because of an internet breach (washingtonpost.com, 2003).

The Federal information Security Management Act of 2002 imposed a mandatory set of procedures that must be followed for all information programs used or operated by anyone associated with a government agency. These processes must follow all Federal Information Processing Standards (FIPS) and other legislation that applies such as, but not limited to, the Privacy Act of 1974 and the Health Insurance Portability and Accountability Act" (HIPAA) (Compliance Home, 2010).

2.2.2 Current Government Legislation

2.2.2.1 NIST and FIPS

An example of a large scale ISP is the Federal Information Processing Standards (FIPS) Publications which is a set of guidelines that are mandatory for all government agencies and are issued by National Institute of Standards and Technology (NIST). The purpose of these documents is to (Commonwealth of Massachusetts, 2010):

- Ensure security and confidentiality of customer information;
- Protect against anticipated threats that would compromise security/integrity; and,
- Protect against unauthorized access.

While these are for federal governmental use and are not intended to be applied in the private sector, they may be used as a reference for Nantucket. The Secretary of Commerce passed the Information Technology Management Reform Act which approved these standards for use. These standards are formed by NIST when "there are compelling Federal requirements and there are no existing voluntary industry standards," (NIST, 2008). This essential means that NIST utilizes FIPS for "filling in the gaps" to form a complete set of standards that completely cover all aspects of information security.

All federally controlled departments and organizations must adhere to the minimum requirements for federal information and information systems. Currently there are seventeen minimum requirements that must be fulfilled to comply with NIST policies

Table 1: NIST Minimum Requirements
Access Control
Awareness and Training
Systems and Communications Protection
Audit and Accountability
Certification, Accreditation, and Security
System and Service Acquisition
Assessments
Contigency Planning
Systems and Information Integrity
Configuration Management
Incident Response
Maintenance
Identification and Authentication
Media Protection
Physical and Environment Protection
Planning
Risk Assessment

Table 1shows the requirements that are crucial to achieving and maintaining information security within an organization (Gutierrez, 2006).

2.2.2.2 ISO/IEC 27000 Series

While 201 CMR is considered the state standard for Massachusetts, the International Standards Organization/International Electro-technical Commission (ISO/IEC) 27000 is considered the industry standard, although it can be applicable to all entities. The ISO/IEC 27000 series is a set of documents that form an Information Security Management System (ISMS). "The ISMS family of standards is intended to assist organizations of all types and sizes to implement and operate an ISMS," (ISO/IEC, 2009). In order to have a successful implementation of an ISP the following principles need to be recognized:

- Awareness for the necessity of information security
- Assignment of responsibility
- Active prevention and detection of information security risks
- Ensuring a comprehensive approach to management and the creation of plausible and achievable policies and procedures that can be followed by personnel
- Commitment from employees at all levels to follow policies and procedures
- Continual reassessment of ISP and modifying where appropriate as threats alter over time (ISO/IEC, 2009)

This list will help give a standard set of guidelines to incorporate into Nantucket's ISP. Information security can be broken down into three main dimensions (ISO/IEC, 2009): confidentiality, availability, and integrity. "Information security is achieved through the implementation of an applicable set of controls, selected through the chosen risk management process and managing using an ISMS, including policies, processes, procedures, organizational structures, software, and hardware to protect the identified information assets," (ISO/IEC, 2009). This helps outline the steps that needs to be taken

in order to create a successful ISP. In Nantucket's case, the asset that is being protected is personally identifiable information collected, stored, and retrieved by the different town offices, and surveys will be used as part of a risk analysis to identify the critical areas of concern.

2.2.2.3 201 CMR 17.00 and M.G.L. c 93H/I

The most recent state legislation to be implemented is 201 CMR 17.00 which has been passed, but does not currently apply to Nantucket.

> "The objectives of this regulation are to insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer," (Commonwealth of Massachusetts, 2010).

This is the bases for this proposal. It will be used in accordance with the IT Department on Nantucket to formulate policies and procedures to prevent any type of information breach.

In his overview of 201 CMR 17.00 Anthony (2009) specifies the applications of the security regulations. The state regulations apply to individuals and organizations that are associated with the commerce and there must be a written out plan for intended use of personal information. Under the state regulations, basic training of employees on proper use and handling of personal information is encouraged.

M.G.L c 93H/I is a document that works in accordance with 201 CMR 17 and together they are known as the Massachusetts Data Breach Notification Law. A new guideline that is implemented by these documents is the fact that if a breach occurs, all entities that may have been affected need to be notified "as soon as practicable and

without unreasonable delay," (Commonwealth of Massachusetts, 2010). This is to ensure that all victims of a possible threat to their personally identifiable information are warned and that they should begin to closely monitor their accounts in case a thief gains access and begins the process of siphoning money. If an organization does not show that the proper steps were taken in preventing a breach then it is their responsibility to cover all costs relating to the incident (Murphy Hesse Toomey and Lehane, 2009).

Although this legislation does not currently apply to municipalities, it is subject to change, so it is in the best interest of Nantucket to start forming an ISP in accordance with this document to be proactive so they will not be overwhelmed if the legislation does get passed.

2.3 The components of the ISP

With personal information at risk in this technology-based society, a comprehensive defense against security breaches is needed. The most effective of which is an Information Security Program (ISP). According to the Massachusetts Enterprise Information Security Policy, a template for a comprehensive ISP, an ISP is:

> "…a management system that represents the policies and controls implemented within an organization. An effective management system provides both management and users with a detailed understanding of the goals, approach and implemented controls for securing the organization's information assets, including but not limited to sensitive information (for example, personal information), and must address the ISP lifecycle; including risk assessment, risk treatment, selection and implementation of security

controls, ongoing evaluation and maintenance" (Commonwealth of Massachusetts, 2010).

According to Sorcha Diver (2006) and the **S**ysAdmin, **A**udit, **N**etworking, and **S**ecurity (SANS) institute, a group devoted to computer security training, the purpose of an ISP is to:

- Protect users and user information;
- Set rules for expected behavior of users, personnel and administrators;
- Authorize security personnel to investigate security incidents;
- Define and authorize the consequences for violation of guidelines;
- Help minimize risk of security incidents; and, to
- Help track compliance with regulations and legislation.

Information Security policies vary among organizations based on the type of information that needs to be secured but the general framework is the same. They must address many issues and policies. To understand a comprehensive ISP, it is important to understand the life cycle of the ISP process and all the components there-in.

ISPs vary widely depending on the type of organization, the amount of resources available and the amount of sensitive information handled. Consequently, there is no generic form of an ISP; however there are several components that are common to most ISPs (Table 2).

Table 2: Common Components of an ISP

Parts of an ISP	Mass EISP (template)	California ISP guide (template)	Oregon.gov IS plan (template)	Princeton*	California Polytechnic State University	Department of health and human service	SANS Institute	Portland State University
Table of contents	yes	yes	yes	yes	yes	yes	yes	yes
Executive Summary/introduction	yes	yes	yes	no	yes	yes	yes	yes
Purpose and scope	no	no	no	yes	yes	yes	no	yes
Roles & Responsibilty	yes	no	yes	yes	yes	yes	no	yes
Risk Managemnt	yes	yes	yes	no	yes	yes	yes	yes
Statement of Applicability								
Policy Management	yes	yes	yes	no	yes	no	yes	yes
Organizing Information Security	yes	yes	yes	no	yes	no	no	no
Asset Protection/Management	yes	yes	yes	no	yes	yes	yes	no
Human Resource Security	yes	yes	yes	no	no	no	no	no
Physical and Enviromental security	yes	yes	yes	no	yes	yes	yes	yes
Management	yes	yes	yes	no	no	yes	yes	no
Access Control	yes	yes	yes	no	yes	yes	yes	yes
development and maintenance	yes	yes	yes	no	yes		yes	no
Incident Management	no	yes	yes	no	yes		yes	no
Disaster Recovery Management	yes	yes	yes	no	yes	yes	yes	no
Compliance	yes	yes	yes	no	yes		yes	yes
Maintenance	yes	no	no	no	no		yes	no
References	yes	no	no	no	no		yes	yes
AUP	no	yes	no	no	no	yes	no	yes
Privacy	no	no	no	yes	yes		no	yes
awareness training	no	no	no	no	yes		yes	no
policy enforcement	no	no	no	no	yes		yes	yes

Table 2 shows the program elements that are included in eight different examples of Information Security Programs. Many ISPs have some of the same elements, but there is considerable variation between ISPs, and none of the elements is mandatory. The blue row is special case; a statement of applicability is never a public document because it contains an inventory of classified information. Consequently, we have no evidence to indicate which ISPs do or do not include such a statement.

Although there are substantial differences between ISPs, we have identified nine common components of all ISPs which are listed here and described in more detail further down:

1. Risk Management
2. Policy Management
3. Asset Protection/Management
4. Physical and Environmental Security
5. Communications and Operations Management
6. Access Control
7. Incident Management
8. Compliance
9. Training

2.3.1 Risk Management

Risk management is the term given to the process of identifying and controlling security risks. It typically involves three parts: risk assessment, risk mitigation and review.

The assessment part of risk management is an essential step for creation of policy and implementation of security protocols. The purpose of risk assessment is to "identify, quantify, and prioritize risks" (Commonwealth of Massachusetts, 2010) that would affect the security objectives of the organization. This process should be conducted systematically so that potential risks and threats to security can be represented in a quantifiable way. This analysis will show where sensitive information is kept, allowing the ISP to focus more on areas with sensitive or high risk, information. Mapping the storage, usage and flow of information from creation to destruction is an effective way of doing this. Assessing and analyzing the collected data allows the identification of 'risk agents' and vulnerabilities (Curtiss, 2010).

'Risk agents' are the entities that actively attack systems in order steal, corrupt and/or damage information. They are the hackers and spies who steal information and sell to the highest bidder. They are the computer viruses that corrupt hard drives, steal information and jump from system to system; migrating and continuing to infect. Vulnerabilities are the flaws, or weak points, in the security system. Correctly identifying all of these design flaws or gaps in security is essential for the ISP to be effective. A hypothetical example of vulnerability in the system could be a filing cabinet that stores credit card numbers without a lock, or using outdated anti-virus protection software (Curtiss, 2010).

The second step in effective risk management, after a thorough risk assessment is completed, is risk mitigation. This step involves the reduction of identified risks by the creation and implementation of an Information Security program. The ISP will be shaped by the size and scope of the organization, its resources, and the amount of sensitive information it stores or owns (The General Court, 2010). After a successful

implementation of the ISP, reviews are conducted on a regular basis to determine the effectiveness of the ISP. This review is the last step in risk management and its purpose is to identify elements of the ISP that failed to work as planned, and to update them so that they are more effective in the future.

As mentioned before, ISPs vary widely depending on the type of organization, the amount of resources available and the amount of sensitive information handled. Consequently, there is no generic form of an ISP; however there are several components that are common to most ISPs (Table 1).

2.3.2 Policy Management

As mentioned before, the information security program is a management system that represents the written policies and any other procedure or control that is required for information security. The policy management section deals with the written part of the ISP. "Policy management includes development, deployment, communication, updating, and enforcement of agency security policies" (California Office of Information Security & Privacy Protection, 2008).

2.3.2.1 Roles and Responsibilities

One key policy of most ISPs is to define the roles and responsibilities of the different staff members and persons who have access to sensitive information. The Massachusetts Enterprise Information Security Policy (MEISP) suggests that corporations have personnel to develop and implement information security policies and procedures, including an Assistant Secretary for Information technology, a Secretariat Chief Information Officer (SCIO), an Information Security Officer (ISO), an Information

Security Board (ISB), and an Information Technology Department (ITD) (Common Wealth of Massachusetts, 2010).

The roles of the Assistant for Information Technology and the SCIO could be combined into one job. The assistant for IT is responsible for the development and maintenance of the ISP. This includes issuing policies for reporting breaches of security and developing mandatory standards and procedures for the different departments to follow. It will be the assistant's responsibility to ensure that the ISP is adopted efficiently and that all future developments adhere to the rules and regulations of the ISP. This includes the communication and training of personnel on all applicable laws and regulations for users (Commonwealth of Massachusetts, 2010).

The ISO will work under the SCIO and their role as a security officer is to ensure that the policies of the ISP are followed by all applicable departments and persons. They are to maintain required documentation and conduct self-audits of the IT department annually to ensure that the ISP is effective and up-to-date. Lastly, it is suggested that an ISP is formed. They are an advisory board that will recommend revisions to the ISP and are mainly used for advice and consultation (Commonwealth of Massachusetts, 2010).

2.3.2.2 Statement of Applicability

Although generally kept internal, each organization is usually required to maintain a statement of applicability. This is a documentation of the security controls, resources and information assets that are relevant to information security. An example of information assets would be personal information and its storage location. The specifics of information security objectives and controls, such as documents and software, are defined in the Statement of applicability (Commonwealth of Massachusetts, 2010).

2.3.3 Asset Protection/Management

Typically, this section of an ISP deals with the identification and inventory of information assets. Ownership of information is decided upon and assigned while information is classified by risk and value to the organization. The two most common types of policies that deal with information assets are the Data Classification policy and the Data and Media Disposal policy.

The purpose of the Data Classification policy is to categorize all information that is processed through the organization and to create guidelines and procedures for the generation, access, modification, disclosure, transmission, and destruction for each category of information. Information is classified into three categories. Class I is public information that has minimal security control. Class II information is for official use only, such as departmental memoranda or meeting minutes. Lastly, Class III information is highly sensitive or confidential information, such as personal information, and should be tightly protected and controlled. This element of the IS policy applies to all personnel that come into contact with information and can range from minimal security measures for class I information to the most intricate and detailed procedures for class III information (George Washington University, 2004).

The second policy common to the asset protection section of an ISP is the Data and Media Disposal policy. This policy's role is to ensure that proper disposal methods of sensitive information are followed. The purpose behind these guidelines is to ensure that no sensitive information is intentionally or accidentally leaked. This policy is based on the Data Classification Policy and it defines the proper procedures and methods for disposal based on the classification of information. The county of Sacramento, California describes methods of destruction for both their electronic and paper media and data.

Physical information cannot “practicably be read or reconstructed” while electronic information and media must be destroyed or erased (Groff, 2005).

2.3.4 Physical and Environmental Security

Information Security Policies deal with more than computers and firewalls. Physical, or environmental, security deals with the protocols in place to safe guard physical information assets (Commonwealth of Massachusetts, 2010). For example, paper copies should be held in filing cabinets with locks and there should closed circuit security cameras monitoring areas with confidential information. Some agencies will hire security officers to monitor access and to protect the facilities. Physical Security verifies authorization and ensures that access control is followed for hard copies of information. Lastly, entry and access to facilities are monitored and logged for self-auditing purposes (California Office of Information Security & Privacy Protection, 2008).

2.3.5 Communications and Operations Management

This section of an ISP describes and inventories the security controls used to protect and maintain the system and communications. Some examples of these controls are back-up protection, anti-virus protection and public access protection. However, this is more than a list of software used to protect the network, but the processes of administering and monitoring these technologies in order to ensure proper network function (California Office of Information Security & Privacy Protection, 2008).

Different companies and entities in ownership of sensitive information use a variety of different methods to monitor and maintain their information security policies. According to Michael Whitman, 100% of the companies surveyed used password protection and 97.9% used virus protection software, while only 50% have personnel

accounts auto logoff after a period of inactivity. Also noted in the study 51% reported that they encourage reporting the violation of their ISP and only 45.8% reported that they monitored the computer usage of their companies (Whitman, 2003). Table 2 shows a more complete taxonomy of security controls used by surveyed companies and government agencies. The goal of the recent regulation passed by the Massachusetts *Office of Consumer Affairs and Business Regulations* is for current ISPs to be augmented and improved with more thorough methods and controls of Information Security to meet a higher standard (201 CMR 17.00: M.G.L. c. 93H, 2010).

Table 3: Percentage of organizations using different types of security controls (Whitman, 2003)

Protection Mechanisms	
Use of passwords	100%
Media backup	97.9%
Virus protection software	97.9%
Employee education	89.6%
Audit procedures	65.6%
Consistent security policy	62.5%
Firewall	61.5%
Encourage violations reporting	51.0%
Auto account logoff	50.0%
Monitor computer usage	45.8%
Publish formal standards	43.8%
Control of workstations	40.6%
Network intrusion detection	33.3%
Host intrusion detection	31.3%
Ethics training	30.2%
No outside dialup connections	10.4%
Use shrink-wrap software only	9.4%
No internal Internet connections	6.3%
Use internally developed software only	4.2%
No outside network connections	4.2%
No outside Web connections	2.1%

2.3.6 Access Control

According to the state of California, access control is the "process of controlling access to systems, networks, and information based on business and security requirements" (California Office of Information Security & Privacy Protection, 2008). The overall goal of this section of an ISP is to ensure that employees with proper authorization can access information while those without it cannot. This includes auditing and logging all requests to access information to make sure that users are following policy and to identify those who are not.

2.3.7 Incident Management

The whole goal of an ISP is to reduce the occurrence of breaches of security. However, no matter how state of the art an ISP is, breaches do occur from time to time. Incident Management is required for those cases. A formal policy is used to explain all of the steps that an individual should take in case of a breach of security. It is the responsibility of all peoples and management staff involved to follow these steps which are generally inspired by applicable laws.

2.3.8 Compliance

This section is two sided. First off, it is important to ensure that all of the security policies and procedures are followed properly. An Auditing process is helpful to check up on this. Secondly, the IT department, or whoever is in charge of the ISP, should self-audit the entire system to check compliance with all applicable state and federal laws. Annual review of the ISP is necessary to ensure this (Commonwealth of Massachusetts, 2010).

2.3.9 Training

When an ISP is finally formed, it contains guidelines and actions that need to be followed for the success of the program. This means that all personnel who must adhere

to the program need to be trained on the new policies and procedures. This needs to be done shortly after implementing the ISP to ensure that it is quickly accepted and utilized. In order to be sure the security training will be affective, the following measures should be taken (Information Services, 2005):

- All new users must participate in an approved training program before being granted access to any information resource;
- All users must sign an acknowledgement stating they have read and understand all requirements and that they have participated in a training program;
- A communication system needs to be set up to relay any new updates or changes to the ISP;
- There should be disciplinary actions in place for incompetence in any of these areas or in violation of the ISP; and,
- New employees must go through an introductory training program

The section on training should emphasize the importance of information security and might include some incidents that highlight the potential consequences of a security breach. In the end, the effectiveness of the ISP is greatly affected by the User error. If people aren't properly trained, then mistakes will be made in following the guidelines in place; this will lead to more security breaches. Therefore, it is important that all people that are affected under the ISP are properly and thoroughly trained.

2.4 Personally Identifiable Information (PII)

The most important portion to any ISP is the information that is being protected. Identifying this information should be the first step when creating an ISP. Based on conversations with key staff in the Nantucket IT department, it is evident that the primary

information security concern within the various municipal offices is the collection, access, storage, and disposal of personal information. The definition of person identifiable information (PII) varies widely depending on the type of organization and the state and federal laws that apply to them. Table 3 is a matrix that contains eight sources seen across the top and various characteristics of personal information down the left hand side. The sources come from a variety of sources including universities, state standards, and a large corporation. This matrix was used to determine which attributes should be included in our working definition of personally identifiable information. By including all of the characteristics with more than three positive responses, a list of five attributes can be formed:

- Medical Records
- License #
- Financial or Credit Card Account #
- Tax Records
- Social Security Number (SNN)

Table 4: Personally Identifiable Information Matrix

Sources	Massachusetts	Princeton	WPI IT	201 CMR 17	NIST	Walmart	Savvis	Portland State University
Characteristics/Level	State Standard	University Standard	University Standard	State Standard	Federal Standard	Large Corporations	Business/ Government Agencies	University Standard
Medical Records	yes	no	yes	no	yes	no	yes	yes
Maiden Name	no	yes	no	no	yes	no	yes	no
License #	yes	yes	yes	yes	yes	yes	yes	yes
Financial or Credit Card Account #	yes	yes	yes	yes	yes	yes	yes	yes
DOB	no	yes	yes	no	yes	no	yes	no
Address and Location Information	no	no	no	no	yes	yes	yes	yes
Tax Records	no	yes	yes	no	yes	no	yes	no
Student ID #	no	yes	yes	no	no	no	no	yes
SSN	yes	yes	yes	yes	yes	yes	yes	yes
Signature	no	no	no	no	no	yes	yes	no
Place of Birth	no	yes	no	no	yes	no	no	no
Phone Numbers	no	no	no	no	no	yes	no	no
Personal Characteristics	no	no	no	no	yes	yes (via video cameras in stores)	yes	no
Passport #	no	no	no	no	yes	no	yes	yes

This list (Table 4) was used to form a preliminary definition as it was altered based on data received later from surveys to form a complete and concise definition to be implemented in the ISP for Nantucket's IT Department.

We have outlined the need for an ISP, what an ISP is composed of, the history of information security, and the government legislation that is currently in place to gain a better understanding in the field of information security. We used this background information to assist the Information Technology Department of Nantucket in creating a complete comprehensive information security program. The steps and processes that were taken to accomplish this are outlined in the next section, the methodology.

III. Methodology

The goal of this project was to assist the IT department of Nantucket in the development of a comprehensive Information Security Program, or ISP. Towns generally have not implemented and used ISPs because they either lack the staff and/or resources. Nevertheless, staff members in the Nantucket IT Department recognized that information security is an issue of major concern and, overall, it was in Nantucket's best interest to implement security policies and procedures suggested by the state; specifically, Regulation 201 CMR 17.00 passed by the *Office of Consumer Affairs and Business Regulations*. Our project team accomplished this by completing three main objectives:

1. Summarized current legislation pertaining to ISPs in Massachusetts, identified best practices in government agencies, corporations, and non-profit organizations, and created complete comprehensive working definition of Personal Identifiable Information.
2. Mapped current patterns of information flow within various offices of the Town of Nantucket, from creation to deletion, to identify possible security issues.
3. Developed draft information security policies and procedures that were recommended to the Town of Nantucket.

3.1 Objective 1: Indentifying Regulations and Practices

The first step we took towards accomplishing our goal was to build upon the literature review. We conducted an in-depth analysis of current legislation pertaining to information security as well as a thorough review of different ISPs. From this analysis we were able to develop two matrices about important aspects of our project. One matrix (see Table 3 in the literature review) identifies what items are typically considered to be Personally Identifiable Information (PII) according to eight different ISPs. We focused on PII because this was the main area of concern for the IT Department in the Town of Nantucket. Based on this assessment, we created a working definition for our data collecting purposes. The types of information that we considered PII are:

- Social Security Number
- Financial or Credit Card account number
- Medical Records

- Tax Records
- License Number

In another matrix (see Table 1 in the literature review) categorized the different components of eight different Information Security Programs. This indicated the key themes on which we focused during data gathering and the development of our draft policies for the Town of Nantucket. Our findings from the preliminary analysis helped us develop our survey and interview questions in Objective 2, and the policies that we developed in Objective 3.

3.2 Objective 2: Mapping information flow and security practices

In order to develop a cohesive and reliable ISP for the Town of Nantucket, we needed to map out the flow of information, from creation to deletion, among the various offices under the jurisdiction of the IT Department. This included user activity and the real time location of any and all information on the network. Also included are the town departments, outside agencies, and private users who access the network or any information on the network. In general, we needed to know: Who accesses the town network? What information is accessed? What is that information used for, and what improvements can be made to current system?

Several steps were taken to answer these questions and achieve our objective. We determined what should be classified as sensitive information for the Town of Nantucket and compiled a list of departments and individual users that have access to said sensitive information. We utilized this information to map the flow of information from creation to deletion around the island and between the various departments and employees. From the surveys, we were able to select the more significant departments and gathered more specific details and opinions through interviews of these departments.

3.2.1 Surveys

We started by creating and distributing an electronic survey (see appendix A) to heads of departments and employees of the Town of Nantucket. There were thirty-six surveys sent out and thirty were returned to us. The surveys themselves were self-administered and were not anonymous because our group needed to know the users and departments. This information was used to later conduct interviews and assist in

achieving our objective of mapping the flow of information on Nantucket. However, our group asked permission from the subject to publish their names and responses. The goal of the survey questions was to help guide the design of interview questions for individuals surveyed.

The surveys were created in Adobe LiveCycle Designer and distributed via email to be opened in Adobe Reader 9.0. The surveys were sent to the managers of the departments and we asked them to distribute the survey on to relevant staff. Each recipient was asked to complete survey and submit via email back to the group. Our sponsor, Linda Rhodes, formulated a cover email requesting the participation of everyone to help increase feedback. Each recipient was also asked to forward the survey to any other employees within their respective departments that might have valuable input. Some difficulties that were encountered while creating the survey within Adobe were formatting and distribution. Formatting issues consisted of recording answers and the overall layout of the survey. Distribution issues consisted of ensuring that all recipients had compatible software, specifically Adobe Reader 9.0 or newer in order to open and complete the survey and that correct responses were received. Completed forms of the first surveys when received did not correctly reflect respondents' true answers therefore a reformatting of the survey was necessary and it was redistributed. Both difficulties were overcome with the assistance of members of the IT department of Nantucket. (See Appendix A for a copy of the survey)

3.2.2 Interviews

We conducted seven interviews with the most significant departments who answered our survey. Our group interviewed departments based on the responses we received from the completed surveys. We placed on departments that handle PII and the departments that do not handle PII were omitted because of time restraints and limited resources. Most of the interviews were performed by all three members of the team and included one member of the department who had the most extensive knowledge of how information was accessed and processed within the department. There were several exceptions to this; however, as some interviews were conducted by only two members and others included multiple members of the department being interviewed. When the

interviews were completed, an outline was formulated for each department. Using this outline, a complete set of summaries was prepared to be added to our findings.

3.3 Objective 3: Develop draft policies and procedures

After we completed an extensive review of the best practices in the field of information security; and determined the information security in some Nantucket departments was insufficient, we developed an ISP that was recommended to the Information Technology (IT) Department for the Town of Nantucket. This ISP included preventative measures to safeguard against anticipated threats, guidelines and procedures to be followed by employees, and policies to address specific areas of interest. Examples of these policies:

- Password Policy
- Backup and Recovery Policy
- Antivirus Policy
- Remote Access Policy
- Wireless Security Policy
- Data Classification Policy
- Computer Data and Media Disposal Policy

The data gained from surveys and interviews was utilized to map the information flow between departments and to tailor the policies to best meet the needs and concerns of the IT Department and the individual departments covered by the policies. We consulted with the IT staff continuously during this phase to ensure the focus of the project was kept on the most crucial aspects. The ISP was formulated in accordance with the IT department, current government legislation, and information gathered on the island. It included all the components that were essential for a successful protection scheme. It was decided, with the assistance of the IT department, that separate policies would be the best approach to make a clear and complete ISP. Each policy followed a consistent format and included the following components:

- Overview
- Purpose

- Scope
- Actually Policy
- Definitions
- Document History

To finish the project, our completed draft of our ISP was presented to the IT Department as a recommendation for future implementation.

IV. Findings

By analyzing the information gathered from our surveys and interviews, we developed the following findings concerning the security of personal information within the town departments of the Town of Nantucket. Through these findings our group drafted multiple policies for the Information Technology of the Town of Nantucket to implement. These policies are presented in Appendix C below.

4.1 Administration Office

The Administration Office has fifteen main duties outlined in the Charter for the Town of Nantucket, which range from supervision of Town departments to preparation of the annual budget and warrants for Town Meeting(s) to implementation of policy as set forth by the Board of Selectmen. All departments, except for the School, Airport and Water Departments, are within the purview of Town Administration. Although the Town Administration does not maintain PII, PII may be brought to the attention of the Town Administration. Therefore, it is important that all policies drafted maintain the security of information that is viewed by any department.

Feedback our group received from our surveys revealed that an area of needed improvement to current information security practices is written policies outlining proper storage and disposal protocols. Currently, there are default practices in place among town departments as to how each department stores and disposes of various media; however, there are no written policies to regulate these practices. The Town Administration disposes of its own media by shredding documents pending approval from the state Public Records Office.

4.2 Assessor

The purpose of the Assessor's Office is to "collect, compile, and verify data for the valuation of all real estate and personal, residential, commercial, and open space property"(Annual Report 29). The Assessor's Office collects and stores Social Security Numbers (SSN) which are kept for two years along with tax records in the event an individual makes a tax appeal. The Assessor's Office is in the process of converting all files to electronic form via, however, they still store a substantial amount of records in locked cabinets and locked storage units off site. Through both the survey results and the interview the Assessor's Office demonstrated a strong set of security practices and roles and responsibilities.

4.3 Building Dept.

The Building Department's duties "include Building, Zoning Enforcement, Plumbing, Gas and Wiring" (Annual Report 61). Survey responses did not provide sufficient information to report on. In consultation with the IT Department, we determined an interview was not needed.

4.4 Conservation Commission

The Nantucket Conservation Commission is regulated by Massachusetts state law to protect Nantucket Island's natural resources. The Conservation Commission does not collect, store, dispose or come in contact with personal information. In consultation with the IT Department, we determined an interview was not needed.

4.5 Council on Aging

The Council on Aging is responsible for various services offered to elderly residents of the Town of Nantucket to enrich living conditions. Our group received drafted policies from the Council on Aging to help guide our drafting of policies for the IT Department. This department has a minimal amount of PII and does not require many improvements. Files and records (Tax and medical) that are maintained by this department are stored in a locked filing cabinet within the offices. Other PII such as SSN and License Numbers are maintained by Human Resources and the Payroll Offices. Feedback from the survey showed that records are stored on the server and in locked cabinets and that all records that have been deemed unnecessary are promptly shredded and disposed.

4.6 Department of Public Works (DPW)

DPW is responsible for a wide variety of public service; some examples are maintenance of roads, waste management, recycling and urban forestry. The DPW consists of 35 full time employees. Of all the employees, 95% do not access computers within their line of work. The only four employees that have computer access and therefore access to the server are the Director, Assistant Director, and two other office specific employees. During the course of our research our group discovered areas of possible improvement. Some improvements that can be made include the process for requesting software and equipment, the physical security of the DPW server, and work related web access. During our interview with the DPW it was stated that the physical security and environment that the server is located in could be improved.

4.7 Finance

The Finance Department "manages vendor payments, manage property and liability insurance coverage, and claims for the Town, County, Land Bank and NRTA. Finance also maintains the budget and accounting records for all fund and account groups" (Annual Report 32). Based on survey results and a follow up interview the Finance Department all PII that is collected and stored by the Finance department is either stored in a vault or on the server. A topic of discussion during our interview with employees from the Finance department was the implementation of annual training for the proper handling of PII and roles and responsibilities of employees in the department.

4.8 Information Technology

The Information Technology (IT) Department "is responsible for implementing and maintaining the technology infrastructure and computing environment for the Town of Nantucket" (Annual Report 23). Another responsibility the IT department is responsible for is the disposal of all electronic media, such as hard drives, of departments they maintain. An improvement that the IT Department would like to see implemented is the development of maintenance windows to display on all servers to improve regular updating procedures. Feedback from surveys also revealed that better physical security of the network servers is also a priority. These servers are situated in the IT department offices and are potentially accessible by any individual within the building. Currently all information that is passed through the IT department is in electronic form and is stored on the network servers. A formal interview was never conducted to because our group was working alongside the IT department during the whole project.

4.9 Health Dept.

The Health Department is responsible for the communication of health issues to the community. In recent times this has mostly consisted of addressing public health issues such as the H1N1 flu virus, tick borne disease, and septic systems inspections. Our research has revealed that the Health Department does not collect, store, or come in contact with PII. No improvements were suggested by this department.

4.10 HDC

The Historical District Commission (HDC) is responsible for "the preservation and protection of historic buildings, places and districts of historic interest" (Annual Report 79). The HDC reviews any and all exterior architectural features of all structures proposed to be altered, moved, constructed, or demolished primarily in the downtown area of the Town of Nantucket. Through survey responses and an interview it was revealed that the HDC does not come in contact with PII, however, some suggestions for improvements included better password practices and implantation of employee training on handling PII.

4.11 Human Resources

The Human Resources (HR) Department is responsible for the maintenance of employee files. These files mainly consist of employee reviews, enrollment in Barnstable County Retirement Association and health insurance enrollment. Our group was unable to conduct a follow up interview with a representative from HR due to scheduling conflicts.

4.12 Human Services

The Council for Human Services (CHS) is responsible for ensuring that all human service needs are addressed. Examples of their duties include issuing food stamps, fuel assistance, insurance enrollment, and various emergency needs (Annual Report 57). Our survey results showed that the CHS collects and stores PII within filing cabinets and that an improvement that can be made is the security of those filing cabinets. In consultation with the IT Department, we determined an interview was not needed.

4.13 Marine and Coastal Resources Department

The Marine and Coastal Resources Department (Marine) is responsible for safety of boaters and all marine traffic in and around the island. For all boater registration and permits Marine collects SSN, date of birth, and residential address which is all stored on electronic servers and in file cabinets. Some improvements suggested in a submitted survey were to devise a better way to secure information and regulate access on a more need to know basis. In consultation with the IT Department, we determined an interview was not needed.

4.14 Our Island Home

Our Island Home (OIH) is a nursing facility that operates as a department of the Town of Nantucket. It provides long term care to town residents which consist of inpatient services, adult day care, and outreach programs. Through survey responses and an interview with the administrative staff, OIH displayed strong practices in regards to securing PII for which they collect, store, and dispose of. OIH utilizes password protection and lock and key security measures for all forms of PII. OIH also has strict

access policies in place in regards to roles and responsibilities. In terms of disposing of records, all hard copy files are promptly shredded by staff and when necessary hard drives and backup tapes are delivered to IT department to be disposed of.

4.15 Park & Recreation

The Park and Recreation Department is responsible for the maintenance of all athletic facilities, including athletic fields and tennis courts of the Town of Nantucket. Our group did not receive a survey or conduct an interview with any representative from The Park and Recreation Department.

4.16 Planning/NP & EDC

The Nantucket Planning Board is responsible for the layout and the granting of permits for construction of roads and structures. Our findings from surveys our group received from representatives from the Planning Board showed that the department does not collect, store and/or dispose of PII. In consultation with the IT Department, we determined an interview was not needed.

4.17 Town Clerk

The Town Clerk's office is responsible for maintaining town meeting minutes and various town registries, primarily voter registration. From the information they gather they publish the "Town of Nantucket Street List" which contains residents' names, addresses, and date of births. The extent of security measures in place are standards setup by the IT department. Feedback during the interview with a representative revealed that

the majority of records maintained by the Town Clerk's office is in hard copy form and that there is little need to convert to electronic form.

4.18 Visitor Services

The Visitor Services "was established to provide a quality experience for Island visitors and residents" (Annual Report 73). The only information that this department comes in contact with is residential addresses, however, representatives who responded to our survey suggested that any policy developed be signed by the parties that it applies to. In consultation with the IT Department, we determined an interview was not needed.

4.19 Wannacomet Water Company

The mission statement for the Wannacomet Water Company is "to provide high quality drinking water that exceeds all established Federal and Commonwealth drinking water standards…educate and inform the public" (Annual Report 76). The Water Company collects necessary customer information and stores all files electronically on server monitored by IT department and all hard copies are shredded. The only suggested improvement by the representatives of the Water Company is to reduce the frequency of password changes.

4.20 Zoning Board of Appeals

The Zoning Board of Appeals grants variances and special permits and decide on appeals in relation to zoning bylaws. Survey findings showed that this department does not come in contact with PII in any form. In consultation with the IT Department, we determined an interview was not needed.

V. Conclusions & Recommendations

Our group began the process of collecting information by distributing a total of thirty-six (36) surveys sent electronically via email. Of those surveys distributed we received thirty (30) completed surveys, 83.3% recipients of the survey responded. Departments that responded were: Assessor's Office, Building Department, Conservation Commission, Council on Aging, Finance Department, HDC, Health Department, HR, Human Services, IT, Marine, Visitor Services, OIH, Planning Board, DPW, Town Clerk, Town Administrator, Wannacomet Water Company, and the Zoning Board. From those responses our group contacted individuals in the various departments that, in consultation with the IT Department, we determined would be valuable sources to question further.

5.1 Password Policy

Based on the survey results and feedback from our interviews, we conclude that the frequency of changing a password for user login to the server was too high. Many employees from town departments stated that at one point in time they were required to change their passwords every 30 days. During the interviews, we inquired about the use of two lengthier password ages, 60 or 90 days. All employees interviewed agreed that a password age of 90 days per password change was reasonable and not overwhelming.

Recommendation: Based on feedback from the departments, we recommend that the password age defined within the drafted Password Policy be set at 90 days.

5.2 Server Security

Another common concern expressed in survey results and interviews was the overall physical security of servers at the town offices. Many of the offices have their

servers located in common areas accessible to any employee. Some offices do have their server's located behind a locked door which is sufficient; however there is still room for security breaches to occur and allow for the server to become unsecure.

Recommendation: We recommend that the Nantucket ISP require that all rooms containing servers be locked at all times and access restricted to administrators.

5.3 Training

Based on the survey results and feedback from our interviews, specifically with Finance, HDC and OIH, we conclude that there is a lack of training for current and new employees within town departments. Each department had a different way of training employees. Some presented a simple power point, where others just trained proactively in a working environment.

Recommendation: In order to correct this, our group recommends that a generic training method be implemented to educate current and new employees in the proper handling of personal information and steps to take to ensure the continual security of said information. This generic training should be instituted as an annual seminar to act as a refresher course and as a meeting to discuss recent issues that have arisen. To ensure the retention of all material discussed a quiz should be required to be completed upon finishing the course. The quiz's focus should be to quantify the overall effectiveness of the course and not be a graded supplement

5.4 Internet Access

Internet access restrictions have been a hindrance among several town offices. From the feedback we received from completed surveys and interviews many town

departments' work is interrupted by restrictions placed on website accessibility. The strict access that is in place by the IT department slows productivity of the town offices because the town offices must request permission to access specific sites and all related links. Through discussion with the IT department we discovered that a new program called Surf Control is in the process of being tested and hopefully implemented in the near future that would help regulate access to work related sites better.

Recommendation: We recommend that less restriction be placed on employee access to the internet. This would help alleviate the tedious process of seeking and granting access.. In addition, if the Surf Control program is implemented then the IT department could potentially cater web access to specific sites to individual departments or potentially individual users.

5.5 Help Desk/User Request

A problem seen among various departments was the lack of prioritizing general IT needs town departments have. Each department prioritizes tasks differently based off their type of business, therefore a system in which departments can categorize the importance of a technical issue.

Recommendation: We recommend the IT department create an online application by which each department can request IT assistance, place a level of priority on the request, and a detailed description of the issue. This application would both benefit the departments and the IT department. The application would benefit the town departments because they would receive faster and more effective service.. The application would benefit the IT department because they would be able to keep track of requests and set priorities more easily.

Finally, based on the risk assessment that we have conducted through interviews and surveys, as well as the lessons learned from best practices elsewhere, we have drafted a comprehensive ISP that is tailored to the nature of the security risks and the needs of the different town departments (see Appendix C). We recommend that the IT department refine these policies and begin implementing them as soon as possible in order to protect the security of Personally Identifiable Information in the various town departments.

References

Anthony, B. (2009, November 9). *Massachusetts data security regulations: new rule and old lessons*. Retrieved from www.nskinc.com/./MA_Data_Security_Regulations_New_Rules_and_Old_Lessons.pdf

Associated Press. (2009, February 9). Identity theft up, but costs fall sharply. *Cbs News*, Retrieved from http://www.cbsnews.com/stories/2009/02/09/business/main4785402.shtml

Baskerville, R and Siponen, M. (2002), "An information security meta-policy for emergent organizations", *Journal of Logistics Information Management*, Vol. 15 Nos 5/5, pp. 337-46.

Billion-dollar love bug worm marks sixth anniversary. (2006, May 4). *Techweb*

Bryes, E. Lowe, J (2004). The Myths and facts behind cyber security risks for industrial control systems. Retrieved from http://www.nealsystems.com/downloads/Myths%20and%20Facts%20for%20Control%20System%20Cyber-security.pdf

Bulgurcu, B, Cavusoglu, H, & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34(3)*

California Office of Information Security & Privacy Protection. (2008, April). *Information security program guide for state agencies*. Retrieved from http://www.cio.ca.gov/OIS/Government/documents/pdf/Info_Sec_Program_Guide.pdf

California Polytechnic State University. (2010, October 5). *Cal poly information security policy*. Retrieved from http://security.calpoly.edu/docs/policy/isp.pdf

Compliance Home. (2010). *Federal information security management act (fisma)*. Retrieved from http://www.compliancehome.com/topics/FISMA

Chronology of data breaches. (2010). Retrieved from http://www.privacyrights.org/data-breach

201 CMR 17.00: M.G.L. c. 93H, 2010 - http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf

Commonwealth of Massachusetts. (2010). *Information security policy*. Retrieved from http://www.mass.gov/?pageID=afterminal&L=5&L0=Home&L1=Research+%26+Technology&L2=IT+Policies%2C+Standards+%26+Guidance&L3=Enterprise+Policies+%26+Standards&L4=Security+Policies+%26+Standards&sid=Eoaf&b=terminalcontent&f=itd_policies_standards_A_InfoSec_ITD-SEC-1-2&csid=Eoaf

Cowan, D. (2010, September 15) How many police officers does it take to email 10,000 criminal records to a journalist by accident? Retrieved from http://www.gpsj.co.uk/view-article.asp?articleid=303

Curtiss, G. (2010). *Iso 27001 - training implementation guide part 1*. Retrieved from http://www.realismssoftware.com/sites/default/files/iso-27001.pdf

Diver, S. (2006) Information security policy- a development guide for large and small companies. *SANS institute InfoSec Reading Room.* Retrieved from http://www.sans.org/reading_room/whitepapers/policyissues/information-security-policy-development-guide-large-small-companies_1331

*The Economist. (*2005, December 10) Fighting fire with fire; computer viruses. Retrieved from http://www.lexisnexis.com/hottopics/lnacademic/

Electronic Privacy Information Center. (2010). *Computer security act of 1987*. Retrieved from http://epic.org/crypto/csa/

Eriksson, J. & Giacomello, G. (2006). The Information revolution, security, and international relations. *International Political Science Review, 27*(3), retrieved from http://www.jstor.org/stable/20445053?seq=5

Federal Trade Commission. (2007, June 25). *Privacy act of 1974, as amended*. Retrieved from http://www.ftc.gov/foia/privacy_act.shtm

General Court. (2010). General Laws. Retrieved from http://www.malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93h

Groff, P. (2005, December 12). *Consumer information disposal policy*. Retrieved from http://www.itpb.saccounty.net/coswcms/groups/public/@wcm/@pub/@itpb/documents/webcontent/sac_004572.pdf

Gutierrez, C. (2006, March). *Minimum security requirements for federal information and information systems*. Retrieved from http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

The History of identity theft. (2009). Retrieved from http://www.spamlaws.com/id-theft-history.html

Hunton & Williams LLP. (2010). New Jersey supreme court's ruling advances employee privacy. *Privacy and Information Security Law Blog*, Retrieved from http://www.huntonprivacyblog.com/2010/04/articles/state-law/new-jersey-supreme-courts-ruling-advances-employee-privacy/

Information Services. (2005, April 20). *Security training policy*. Retrieved from http://www.med.wayne.edu/hipaa/policies/security/MSIS%20Policy%20Binder/Section%2001%20-%20Policies/Tab%2008%20-%20Security%20Training%20Policy/Security%20Training%20Policy.pdf

Jackson, B. (2009, March 23). *Massachusetts data breach laws.* Retrieved from http://www.sourceconference.com/bos09pubs/BJackson%20-%20MADataBreachLawsRegsandResponsibilites.pdf

Klein, A. (2010). 18- to 24-year-olds most at risk for id theft, survey finds. *The Washington Post*, Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2010/03/16/AR2010031604209.html

Ma, Q, Johnston, A, & Pearson, J. (2008). Information security management objectives and practices: a parsimonious framework. *Information Management and Computer Security, 16*(3), 251-70.

Massachusetts Government. (2009, April 1). *Information security policy*. Retrieved from http://www.mass.gov/?pageID=afterminal&L=5&L0=Home&L1=Research+%26+Technology&L2=IT+Policies,+Standards+%26+Guidance&L3=Enterprise+Policies+%26+Standards&L4=Security+Policies+%26+Standards&sid=Eoaf&b=terminalcontent&f=itd_policies_standards_A_InfoSec_ITD-SEC-1-2&csid=Eoaf

McCallister, E, Grance, T, & Scarfone, K. (2010, April). *Guide to protecting the confidentiality of personally identifiable information (pii)*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

McLean, B, & Elkind, P. (2003). *The smartest guys in the room: the amazing rise and scandalous fall of Enron*. New York: Penguin Group

Murphy Hesse Toomey and Lehane. (2009, October). *Data security law mgl chapter 93h and 201 cmr 17.00*. Retrieved from http://www.mhtl.com/assets/PDF/Data-Security-Law.pdf

Office of Information Technology at Princeton University. (2010, October 27). *Policy section on personally identifiable information (pii)*. Retrieved from http://www.princeton.edu/itsecurity/policies/infosecpolicy/pii/

Oregon Government. (2010). *Information security plan*. Retrieved from http://www.oregon.gov/DAS/EISPD/ESO/SecPlan/Plan.doc

Portland State University. (2009, November 19). *Information security policy*. Retrieved from http://www.oit.pdx.edu/dev/files/infosec_policy_final_111909.pdf

Princeton University. (2008, April 7). *Information security policy*. Retrieved from http://www.princeton.edu/itsecurity/policies/InfoSecPolicy.pdf

Privacilla. (2001, March 07). *The computer matching and privacy protection act.* Retrieved from http://www.privacilla.org/government/cmppa.html

Richardson, R. (2008). *CSI Computer & security survey.* Retrieved from http://www.cse.msstate.edu/~cse6243/readings/CSIsurvey2008.pdf

SANS Institute. (2004). *The many facets of an information security program*. Retrieved from http://www.sans.org/reading_room/whitepapers/awareness/facets-information-security-program_1343

Savvis. (2008, August). *Personally identifiable information*. Retrieved from http://www.savvis.net/en-US/Info_Center/Documents/WP_Personally%20Identifiable%20Information%20-%20v1.6_20080820.pdf

Sovern, J. (2004). Stopping identity theft. *The Journal of Consumer Affairs*, 38(2), retrieved from http://onlinelibrary.wiley.com/doi/10.1111/j.1745-6606.2004.tb00866.x/pdf

Stoneburner, G, Goguen, A, & Feringa, A. (2002). Risk management for information technology systems. *National Institute of Standards and Technology*.

Sullivan, S. (2000). How I lost my good name. *The New York Times*, Retrieved from http://www.nytimes.com/2000/04/17/opinion/how-i-lost-my-good-name.html

"Town of Nantucket Annual Report".2009.

US Department of Health and Human Services. (2010, July 19). *Overview HIPPA*. Retrieved from https://www.cms.gov/hipaageninfo/

US Department of Health and Human Services. (2005, July 19). *Information security program*. Retrieved from http://www.samhsa.gov/IT/Docs/Information_Security_Program_Policy_07192005.pdf

Wal-Mart. (2010, February 23). *Wal-Mart privacy policy*. Retrieved from http://walmartstores.com/PrivacySecurity/9243.aspx#infoWeCollect

Washingtonpost.com. (2003, May 16). *Timeline: the U.S. government and cyber security*. Retrieved from http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A50606-2002Jun26¬Found=true

Whitman, M. (2003). Enemy at the gate: threats to information security. Communications of the ACM, 46(8), retrieved from http://delivery.acm.org/10.1145/860000/859675/p91-whitman.pdf?key1=859675&key2=3792455821&coll=GUIDE&dl=GUIDE&CFID=106186210&CFTOKEN=75823256

Wisegeek.com, (2010). What is financial fraud? Retrieved from http://www.wisegeek.com/what-is-financial-fraud.htm

Worcester Polytechnic Institute. (2010). Acceptable use policy. Retrieved from http://www.wpi.edu/offices/policies/aup.html

Appendix A: A Survey of Town Departments

WPI Student Project
Fall Semester 2010
Developing an Information Security Program (ISP) for the Town of Nantucket

This survey is being conducted by three students from WPI on behalf of the Town of Nantucket IT department to map the flow of information and the security of that information. The survey is confidential, and the results will be used to help improve information security within town offices. As a follow up to this survey individuals may be contacted to participate in an interview conducted by the students. Individuals will not be quoted without their prior approval.

USE DESKTOP OUTLOOK CLIENT FOR SEND /RECEIVE OF THIS PDF. DO NOT SAVE THE FILE. COMPLETE FORM AND CLICK SUBMIT BUTTON AT THE TOP RIGHT OF FORM.

Personally Identifiable Information (PII) can be any information that can identify an individual. This does not include publicly available information like your name or your phone number. With this being said, there may be some grey areas where one cannot be sure if it falls under PII or not. For this reason we have developed our working definition of PII to clarify what exactly it contains. The following traits are all considered PII for our purposes:

- Medical Information
- License #
- Financial or Credit Card Account #
- DOB
- Address and Location Information
- Tax Records
- SSN

Information Security Survey

Date:	
Name:	
Department:	
Job Title:	

1) Does your department collect, store, or access PII?

◯ Yes ◯ No

2) Please indicate whether you agree or disagree with the following statements.

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
a) The Town of Nantucket should have formal procedures for protecting PII.	◯ SD	◯ D	◯ N	◯ A	◯ SA
b) HR should conduct background checks on new hires or transferred employees if they are to have access to PII.	◯ SD	◯ D	◯ N	◯ A	◯ SA
c)All employees and contractors with access to PII should be required to sign a confidentiality agreement.	◯ SD	◯ D	◯ N	◯ A	◯ SA
d) All employees and contractors with access to PII should be given training on information security policies and procedures.	◯ SD	◯ D	◯ N	◯ A	◯ SA
e) Departmental job descriptions should clearly indicate the information security responsibilities of the position.	◯ SD	◯ D	◯ N	◯ A	◯ SA
f) There should be consequences for sharing passwords, poor practice of protecting passwords, and not creating strong passwords.	◯ SD	◯ D	◯ N	◯ A	◯ SA

3) What security measures are in place to protect PII? (Check all that apply)

◯ Locking File Cabinet ◯ Media Backup ◯ Virus Protection ◯ Other (Write on Separate Lines)

◯ Computer Passwords ◯ Web Access Restrictions ◯ Peer Incident Reporting

◯ Firewall ◯ Employee Training ◯ Clear Policies

4)Does your department maintain records of who accessed what PII and when?

◯ Yes ◯ No

5) Please fill in the table below to the best of your ability. If you do not handle any of the types of PII disregard the other boxes for that row.

PII Type	How is this information accessed? (e.g. server, e-mail)	What is this information used for? (e.g. payroll, employee review)	Where is this information stored? (e.g. server, file cabinet)
Social Security Numbers			
License Number			
Financial and/or Credit Card Account Number			
Date of Birth			
Residential Address			
Medical Records			
Tax Records			

6) Does your department dispose of their own media containing PII? (e.g. CD, hard drives, paper files etc.)

◯ Yes ◯ No

If you answered YES to Question 6 please briefly explain what disposal methods are used in the text box below.

7) Do you have a Town-issued laptop?

◯ Yes ◯ No

If you answered YES to Question 7 please indicate if you store PII on this laptop.

◯ Yes ◯ No

8) Do you store PII on any external devices. (e.g. USB flash drives, external hard drives, PDAs etc.)

◯ Yes ◯ No

9) How could the security of PII be improved in your department?

Appendix B1: Table of Survey Responses

Table 5: Yes/No responses from survey by department

Department	Handles PII?	Maintain records of who accessed what PII and when?	In-house disposal of records?	Town Issued Lap-tops?	PII on laptops?	PII on External Devices?
Administration	yes	no	yes	no	no	no
Assessor	yes	no	yes	yes	no	no
Building Dept	yes	no	yes	no	no	no
Conservation Comission	yes	no	yes	no	no	no
Council on Aging	yes	no	yes	no	no	no
DPW	yes	no	no	yes	no	no
Finance	yes	no	yes	yes	no	no
Information technology	yes	no	no	yes	no	no
Health Dept	yes	no	no	yes	no	no
HDC	yes	no	yes	yes	no	no
Human Resources						
Human Services	yes	yes	no	no	no	no
Marine	yes	yes	no	no	no	yes
Our Island Home	yes	no	yes	yes	no	no
Park&Rec						
Planning/ NP &EDC	no	no	no	no	no	no
Town Clerk	yes	no	no	yes	no	no
Visitor Services	yes	no	yes	yes	no	no
Wannacomet Water	yes	yes	yes	yes	no	no
Zoning Board of Appeals	no	no	no	no	no	no

Appendix B2: Survey Responses of Security Measures

Table 6: Survey results for current security measures in place by department

Department	Locking File Cabinet	Media Backup	Virus Protection	Computer Passwords	Web Access Restrictions	Peer Incident Reporting	Firewall	Employee Training	Clear Policies
Administration	yes	yes	yes	yes	yes	no	yes	no	no
Assessor	yes	no	no	no	no	no	no	yes	no
Building Dept									
Conservation Comission									
Council on Aging	yes	yes	yes	yes	yes	yes	yes	yes	yes
DPW	no	no	yes	yes	yes	no	yes	no	no
Finance	yes	yes	yes	yes	yes	no	yes	no	no
Information technology	yes	yes	yes	yes	yes	no	yes	no	no
Health Dept	no	yes	yes	yes	yes	no	yes	no	no
HDC	no	no	no	yes	yes	no	no	no	no
Human Resources									
Human Services	yes	no	yes	yes	yes	no	no	no	no
Marine	yes	no	no	yes	no	no	no	yes	no
Our Island Home	yes	yes	yes	yes	yes	yes	yes	yes	yes
Park&Rec									
Planning/ NP &EDC	yes	no	no	yes	no	no	no	no	no
Town Clerk	no	no	no	yes	no	no	yes	no	no
Visitor Services	no	no	yes	no	no	no	no	no	no
Wannacomet Water	no	yes	yes	yes	yes	no	yes	yes	no
Zoning Board of Appeals	no	yes	no	yes	yes	no	no	no	no

Appendix C: Drafted Policies

Within Appendix C are all the policies that our group, in collaboration with the IT Department, drafted along with policies already drafted by the IT department prior to our arrival on Nantucket. These policies were created using information gathered from surveys, interviews and samples from preexisting ISPs. All of these policies will serve as a foundation for the final ISP implemented throughout town departments indefinitely.

Anti-virus Policy

Overview:

This policy is an internal IT policy which defines anti-virus policy on every computer including how often a virus scan is done, how often updates are done, what programs will be used to detect, prevent, and remove malware programs. It defines what types of files attachments are blocked at the mail server and what anti-virus program will be run on the mail server. It may specify whether an anti-spam firewall will be used to provide additional protection to the mail server. It may also specify how files can enter the trusted network and how these files will be checked for hostile or unwanted content. For example it may specify that files sent to the enterprise from outside the trusted network be scanned for viruses by a specific program.

Purpose:

This policy is designed to protect the organizational resources against intrusion by viruses and other malware.

Anti-Virus Policy:

The organization will use a single anti-virus product for anti-virus, spamware and adware protection and that product is Symantec Client Security. The following minimum requirements shall remain in force.

- The anti-virus product shall be operated in real time on all servers and client computers. The product shall be configured for real time protection.
- The anti-virus library definitions shall be updated at least once per day.
- Anti-virus scans shall be done a minimum of once per day on all user controlled workstations and servers.

No one should be able to stop anti-virus definition updates and anti-virus scans except for domain administrators.

Email Server Policy:

The email server will have additional protection against malware since email with malware must be prevented from entering the network.

Email Malware Scanning

In addition to having the standard anti-virus program, the email server will additionally include Symantec Email Security which will be used to scan all email for malware. This scanner will scan all email as it enters the server and scan all email before it leaves the server. In addition, the scanner may scan all stored email once per week for viruses or malware.

When a virus is found or malware is found, the policy shall be to quarantine the email and to notify the recipient.

Blocked Attachment Types

- The Town of Nantucket Firewall may block emails with some attachments, known to potentially contain active content which may be used to infect a computer with hostile software or because these attachment types are commonly successfully used by virus programs or malware to spread.
- When an email breaks the rules and contains an illegal file attachment, the attachment will be removed and the email allowed through, allowing the receiver to follow up if the attachment was genuine.

Anti-spam Server

To increase mail security, an anti-spam server will examine all incoming email to reduce the load on the mail server introduced by spam and to minimize the potential threats from viruses and other email based threats. Spam and malware definitions will be updated daily. Email positively identified as SPAM will be deleted without notification to sender or recipient. Email that is suspected as being SPAM will be flagged and allowed through to the receiver or quarantined. Quarantined emails will be released to the receiver upon request.

Firewall Policy:

To help prevent hostile software from impacting the Town of Nantucket's computing environment, all systems on the network that connect to the internet of shall be protected by an approved firewall system. These systems shall be under the control of the Town's IT Department. Any systems connecting to the Town's network shall do so by connecting through this firewall system. Such access shall be governed by the Remote User Policy and the Mobile User Policy for the Town of Nantucket.

All systems operating within and outside of the Town of Nantucket's organizational network shall also be protected by an approved local firewall software system whenever connected to the internet.

Any user wishing to connect their computer to the organizational network shall have that computer checked for malware by the Town's IT department prior to making any connection.

Backup and Recovery Policy

Overview:

The Town of Nantucket Information Technology Department is responsible for providing adequate backups to ensure the recovery of electronic information, which includes electronic data and software, in the event of failure, un-intentional and intentional destruction of data or disaster. These backup provisions will allow the Town of Nantucket business processes to be resumed in a reasonable amount of time with minimal loss of data.

Purpose:

This policy describes the processes that will be followed to ensure electronic information is copied onto secure storage media on a regular basis (i.e., backed up), for the purpose of disaster recovery and business resumption. This policy outlines the minimum requirements for the creation and retention of backups. Special backup needs which exceed these minimum requirements will be accommodated on an individual basis. Since failures can take many forms, and may occur over time, multiple generations of backups will be maintained.

Scope:

This policy applies to all electronic information stored on Town of Nantucket owned and supported servers. All Town of Nantucket data accessed from workstations, laptops, or other portable devices should be stored on networked file server drives to the extent possible to assure proper backup.

Federal and state regulations pertaining to the long-term retention of information (e.g., financial records) will be met using separate archive policy and procedures, as determined by the Business Owner of the information, and in accord with the Records Management Program. Long-term archive requirements are beyond the scope of this policy.

Policy:

Backups of all Town of Nantucket data and software must be retained such that computer operating systems and applications are fully recoverable.

- Full backups are performed nightly on Monday, Tuesday, Wednesday, Thursday, and Friday.
- Backups will not be performed on designated Holidays.
- Backups performed Monday through Thursday shall be kept for two weeks and the tapes reused when expired.

- There shall be a separate set of tapes for Fridays of the month such as Friday1, Friday2, etc. Backups performed on Friday or weekends shall be kept for four weeks and the tapes reused the next month on the applicable Friday.
- A special month-end backup of the MUNIS server will be done at the end of each month and kept for twelve months.
- A special year-end backup of the MUNIS server will be done at the end of the fiscal year and retained indefinitely.
- The status of each backup job will be checked each day to ensure successful completion and to correct any issues that may arise.
- The date each tape was put into service shall be recorded on the tape. Tapes that have been used longer than twelve months shall be discarded and replaced with new tapes.
- Tape drives will be cleaned at a minimum, once every 3 months and will be replaced, at a minimum, once a year.
- The ability to restore data from backups shall be tested at least once per 90 days.
- Offline tapes will be stored in the Town Building in a fireproof vault. The latest set of tapes may be held off-site in IT personnel possession in transport to the vault the next business day.
- Users that need files restored must submit a request to the help desk and include information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.
- User account data associated with the file and mail servers will be archived one month after they have left the organization.

Definitions:

Backup - The saving of files onto magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.

Archive - The saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing on-line storage room.

Restore - The process of bringing off line storage data back from the offline media and putting it on an online storage system such as a file server.

Password Policy

Overview:

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the Town of Nantucket's entire network. As such, all Town of Nantucket employees (including contractors and vendors with access to Town of Nantucket systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose:

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

Scope:

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Town of Nantucket facility, has access to the Town of Nantucket network, or stores any non-public Town of Nantucket information.

Policy:

General

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All production system-level passwords must be part of the InfoSec administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days. The recommended change interval is every 60 days.
- User accounts that have system-level privileges granted through group memberships must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All user-level and system-level passwords must conform to the guidelines described below.

General

<u>General Password Construction Guidelines</u>

Passwords are used for various purposes in the Town of Nantucket systems. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Everyone should be aware of how to select strong passwords.

Characteristics of a weak password include:

- Password is shorter than 8 characters.
- Password is a word found in a dictionary (English or foreign)
- Password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words "Town of Nantucket", "Nantucket", or any derivation.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Characteristics of a strong password include:

- Contains both upper and lower case characters (e.g., a-z, A-Z)
- Has digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Is at least eight alphanumeric characters long and is a passphrase (Ohmy1stubbedmyt0e).
- Is not a word in any language, slang, dialect, jargon, etc.
- Is not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

<u>Password Protection Standards</u>

Do not use the same password for Town of Nantucket accounts as for other non-Town of Nantucket access accounts (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various Town of Nantucket access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account.

Do not share Town of Nantucket passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Town of Nantucket information.

Here is a list of "dont's":

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

If someone demands a password, refer them to this document or have them call someone in the Information Security Department.

Do not use the "Remember Password" feature of applications (e.g., Internet Explorer, Outlook, and Firefox).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

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

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

Town of Nantucket Password Requirements (subject to change)

The following password requirements have been set:

- Minimum Length - 8 characters required
- Maximum Length – No limit, although 14 characters is a practical limit
- Minimum complexity - It is strongly suggested that Passwords use three of the following four types of characters:
    - Lowercase
    - Uppercase
    - Numbers
    - Special characters such as !@#$%^&*(){}[]
- Passwords are case sensitive and the user name or login ID is not case sensitive.

- Password history – 5 unique passwords required before an old password may be reused. This number should be no less than 24.
- Maximum password age - 90 days
- Minimum password age - 1 days
- Account lockout threshold - 3 failed login attempts
- Reset account lockout after – 30 minutes.
- Account lockout duration - 30 minutes.
- Password protected screen savers are enabled and should protect the computer within 15 minutes of user inactivity. Computers should not be unattended with the user logged on and no password protected screen saver active. Users should be in the habit of not leaving their computers unlocked. They can press the CTRL-ALT-DEL keys and select "Lock Computer".
- Rules that apply to passwords apply to passphrases which are used for public/private key authentication

Application Development Standards

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

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.
- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

Use of Passwords and Passphrases for Remote Access Users

Access to the Town of Nantucket Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

Enforcement:

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

Definitions:

Application Administration Account Any account that is for the administration of an application (e.g., Munis administrator, Exchange

Remote Access Policy

Overview:

The Town of Nantucket Information Technology Department is responsible for defining and implementing a remote access policy which defines standards for connecting devices remotely to the Town's network. In addition the IT department is also responsible for defining and applying security standards to these approved devices that are to connect to the Town's network. This remote access policy specifies how remote users can connect to the Town's network and the requirements for each device before they are allowed to connect. The Remote Access policy will specify the following.

1. The approved devices that are allowed to connect to the Town's network.
2. The anti-virus program required on remote devices connecting to the network.
3. Firewall requirements on remote devices.
4. The latest Security Updates installed and the device configured for automatic updates to run daily.
5. The method used for remote access to the Town's network once an internet connection has been established will be via a Virtual Private Network.

Purpose:

The purpose of the remote access policy is to define standards for establishing a secure connection to the Town of Nantucket's network from any approved remote device. These standards are designed to minimize the potential exposure to the Town's network infrastructure from damages including the loss of data to critical internal systems such as Email, MUNIS etc.

Scope:

This policy applies to all approved devices that are owned and supported by the Town of Nantucket that will be used to remotely connect to the Town's network. All Town of Nantucket data accessed from workstations, laptops, or other portable devices should be stored on networked file server drives to the extent possible to assure proper backup.

Policy:

- The only approved devices that are allowed to connect remotely to the Town's network are TON owned and supported laptops. The only exception will be for consultants, vendors etc that have their own devices and their job function requires them to connect these devices to the Town's network. Under no circumstances will any of these devices be permitted to connect to the Town's network directly or remotely without the prior review and approval of the IT department.

- The laptop must have the approved version of anti-virus installed, be operating in real time protection mode, and have up to date virus definitions downloaded and installed.
- The laptop must have an approved Firewall installed, enabled and appropriately configured prior to establishing a remote connection to the Ton's network.
- The laptop must have the latest security patches installed from Microsoft and the laptop must be configured to run automatic updates daily.
- Once an active internet connection is established on the laptop the only permitted method to remotely connect to the Town's network will be via a secure PPTP Virtual Private Network connection. A shortcut will be created on each laptop approved for remote access to the TON's network and a user name and a secure passphrase must be provided in order to establish a secure connection. The remote account will be configured on the Firebox and will use MS CHAP V2 authentication and MPPE 128 bit encryption.

Definitions:

Remote Access - The ability to log onto a network from a distant or remote location, generally this implies a computer, a modem, a wireless router and some remote access software to connect to the network.

TON's Network -. The Town of Nantucket's network infrastructure which includes Firewalls, Routers, Switches, Servers (both the physical hardware and the software i.e. the applications that run on, and the data that is stored on them

Firewall – A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.

VPN – An acronym for Virtual Private Network, a network that uses public telecommunications infrastructure such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

PPTP – An acronym for Point to Point Tunneling Protocol, a technology for creating VPN's. Because the internet is essentially an open network, the Point to Point Tunneling Protocol is used to ensure that messages transmitted from one VPN node to another are secure.

MS-CHAP V2 – An acronym for Microsoft's Challenge-Handshake Authentication Protocol. MS-CHAP V2 provides mutual authentication between peers by piggybacking a peer challenge on the response packet and an authentication response on the success packet.

MPPE – An acronym for Microsoft's Point to Point Encryption. MPPE is a protocol for encrypting data across VPN's.

Wireless Security Policy

Overview:

The Town of Nantucket Information Technology Department is responsible for defining and implementing a Wireless Security policy which defines standards for all wireless communications. This policy addresses four major categories of wireless technology implementation as listed below.

Wireless Mobile Communications (WMC) utilize licensed frequencies and include such services as 2G and 3G cellular telecommunications, Cellular Digital Packet Data (CDPD), Global System for Mobile Communication (GSM), and General Packet Radio Services (GPRS), among others. WWANs can span world-wide but are currently limited in data transmission rates, typically from 56Kbps to 300Kbps.

Wireless Local Area Networks (WLAN) include 802.11 (Wi-Fi). WLAN networks utilize unlicensed frequencies and are configured in either *ad hoc* or infrastructure mode. An *ad hoc* WLAN consists of multiple wireless clients communicating as peers to share data without the use of a central Wireless Access Point (WAP). An infrastructure WLAN consists of multiple wireless clients communicating with Wireless Access Point (AP) devices, which are usually connected to a wired network. Devices such as notebook computers or Personal Digital Assistants (PDAs) must generally be within 100 meters of a wireless access point to communicate (100 meters indoors; somewhat longer distances outdoors). New wireless technology is rapidly expanding the useable distances of 802.11 networks to much longer distances. 802.11 networks support fast data communication rates, from 11Mbps to 54Mbps – speeds approaching that of typical wired networks.

Wireless Personal Area Networks (WPAN) such as Bluetooth and Infrared (IR) are generally designed to allow small devices to communicate over a limited distance. Typical WPANs might be used, for example, to wirelessly interconnect a keyboard or headset to a computer, a computer to a projector, a PDA to a notebook computer, or to communicate among PDAs. Bluetooth supports data transmission rates of up to 720Kbps at distances of up to 30 feet.

Wireless Wide Area Networks (WWAN, non-cellular) High-speed point-to-point wireless connections, sometimes called Fixed Wireless to differentiate them from mobile wireless connections or Wireless LANs. For the purposes of this policy document, WWAN networks are defined as those utilizing FCC licensed radio frequencies (microwave) for point-to-point communication between facilities. This section will not apply to client communication or the use of devices operating within unregulated frequencies. Microwave networks support data communication rates from T1 to OC-3 – speeds are very dependent on the frequency, type of radio and protocol(s) utilized.

Purpose:

The purpose of the wireless security policy is to define and implement standards for secure wireless communications between devices, and also to ensure that these standards are designed to minimize the potential risk exposure to the TON's network infrastructure.

Scope:

This policy applies to all wireless communications between approved devices that are owned and supported by the Town of Nantucket that will be used to remotely connect to the Town's network. All Town of Nantucket data accessed from workstations, laptops, or other portable devices should be stored on networked file server drives to the extent possible to assure proper backup.

Policy:

- The only approved devices that are allowed to connect remotely to the Town's network are TON owned and supported laptops. The only exception will be for consultants, vendors etc that have their own devices and their job function requires them to connect these devices to the Town's network. Under no circumstances will any of these devices be permitted to connect to the Town's network directly or remotely without the prior review and approval of the IT department.
- The laptop must have the approved version of anti-virus installed, be operating in real time protection mode, and have up to date virus definitions downloaded and installed.
- The laptop must have an approved Firewall installed, enabled and appropriately configured prior to establishing a remote connection to the Ton's network.
- The laptop must have the latest security patches installed from Microsoft and the laptop must be configured to run automatic updates daily.
- Once an active internet connection is established on the laptop the only permitted method to remotely connect to the Town's network will be via a secure PPTP Virtual Private Network connection. A shortcut will be created on each laptop approved for remote access to the TON's network and a user name and a secure passphrase must be provided in order to establish a secure connection. The remote account will be configured on the Firebox and will use MS CHAP V2 authentication and MPPE 128 bit encryption.

Definitions:

TON's Network -. The Town of Nantucket's network infrastructure which includes Firewalls, Routers, Switches, Servers (both the physical hardware and the software i.e. the applications that run on, and the data that is stored on them

Firewall – A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.

VPN – An acronym for Virtual Private Network, a network that uses public telecommunications infrastructure such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

PPTP – An acronym for Point to Point Tunneling Protocol, a technology for creating VPN's. Because the internet is essentially an open network, the Point to Point Tunneling

Protocol is used to ensure that messages transmitted from one VPN node to another are secure.

MS-CHAP V2 – An acronym for Microsoft's Challenge-Handshake Authentication Protocol. MS-CHAP V2 provides mutual authentication between peers by piggybacking a peer challenge on the response packet and an authentication response on the success packet.

MPPE – An acronym for Microsoft's Point to Point Encryption. MPPE is a protocol for encrypting data across VPN's.

Computer Data and Media Disposal Policy

Overview:
Computer Data and Media Disposal Policy for the town departments of Nantucket that governs the proper procedure and practices for disposing of any media that contains Personally Identifiable Information (PII).

Purpose:

The Town of Nantucket is committed to reducing identity theft and other fraud through protection of PII. This document states the Computer Data and Media Disposal Policy for the Town of Nantucket.

Scope:

These regulations apply to any and all PII that any Town department comes in contact with. This includes collecting, storing, transferring, and/or disposing of PII.

Policy:

It shall be the policy of the Town of Nantucket that PII will be disposed of in such a way that any data is unreadable or incapable of being reconstructed.

Standards in Order to Comply with the Policy:

The standard is one of reasonableness. It requires implementation and monitoring compliance with adopted policies and procedures relating to the destruction of PII. There are a number of accepted methods of document destruction that the information cannot be practicably read or reconstructed:

Paper:

Paper with PII must be disposed of by burning, pulverizing or shredding so that the information cannot practicably be read or reconstructed.

Electronic Media:

Computer equipment that previously contained consumer information must be disposed of by destroying or erasing the information.

A. If erased, the method shall meet the Department of Defense (DO) standards, which states, *"the method of destruction shall preclude recognition or reconstruction of the classified information or material."* All computer equipment shall be tested to ensure information cannot be retrieved.

B. All other media shall have all the consumer information removed (the mechanism may vary depending on the media type) and tested to ensure the information cannot be retrieved.
C. If the media is not "technology capable" of being erased, the media shall be overwritten or destroyed.

Use of third party to dispose of consumer information:

The reasonableness measure standard requires monitoring compliance of any contract with another party who has been contracted to dispose of consumer information. Due diligence must be exercised in monitoring compliance, including:

A. Any contracts entered into with a third party for the purpose of destroying PII shall include language requiring vendors to adhere to the Town of Nantucket Disposal Policy. A copy of the Policy shall be included in the bid solicitation (if applicable) and contract.
B. Reviewing an independent audit of the disposal company's operations and/or its compliance;
C. Obtaining information about the disposal company from references or other reliable sources;
D. Requiring that the disposal be certified;
E. Reviewing and evaluating of the disposal company's information security measures to determine the competency and integrity of the potential disposal company.

Policy Responsibilities:

The following responsibilities are required of Department Heads, IT Department, and general workforce employees.

Responsibilities of Department Heads:

A. Monitor compliance by employees.
B. Ensure that any third party who has been contracted to dispose of PII does so in a manner consistent with this policy and departmental procedures.
C. Ensure that any procedures developed by departments shall be consistent with the Town of Nantucket's Computer Data and Media Disposal Policy and not deviate from the Town standard.

Responsibilities of IT Department:

A. Ensure all hard drives are wiped clean before disposal or reuse.
B. Test hard drives to ensure they are clean.
C. Maintain an inventory and a record of movements of hardware and electronic media such as workstations, servers, or backup tapes.

D. Ensure that any and all indentifying tags, such as names or phone numbers, have been removed.

Responsibilities of Employees:

A. Employees shall follow their department procedures and adhere to Town policy when disposing of consumer information.
B. Protect against unauthorized access to or use of information in connection with its disposal.

Enforcement:

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

Definitions:

Personal Identifiable Information (PII)– refers to information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

Human Resources Security

Overview:
To define the measures to be taken by Human Resources (HR) Department of the Town of Nantucket in regards to protecting personally identifiable information.

Purpose:
The purpose of this policy is to outline steps that the Human Resources Department should take to assist the Information Technology (IT) Department.

Scope:

This policy primarily concerns the HR Department and the IT Department but can be applied to all Town Departments.

Policy:

A. HR must ensure that all new and current employees review all policies outlined in the Information Security Program (ISP) of the Town of Nantucket.
B. HR must immediately notify IT Department upon the hiring of new employees.
C. HR must immediately notify IT Department upon the termination or departure of an employee.
D. During exit interview employee must relinquish any and all town issued equipment.

Enforcement:

Disciplinary actions will be governed by HR policy and carried out by Department Heads and HR representatives.

Mobile Device Policy

Overview:

The Town of Nantucket seeks to protect all mobile devices from unauthorized access, use, disclosure, alteration, modification, deletion, destruction and/or removal.

Purpose:

The purpose of this policy is to describe the minimum security policy for the Town of Nantucket's mobile devices. Mobile devices must be appropriately secured to prevent sensitive or confidential data from being lost or compromised, to reduce the risk of spreading viruses, and to mitigate other forms of abuse of the Town of Nantucket computing and information infrastructure.

Scope:

The scope of this security policy (Mobile Device Security Policy) includes all users of any Town of Nantucket mobile device.

Policy:

1. Whenever possible, all mobile devices must be password protected. Choose and implement a strong password – refer to Password Policy.

2. The physical security of these devices is the responsibility of the employee to whom the device has been assigned. Devices shall be kept in the employee's physical presence whenever possible. Whenever a device is being stored, it shall be stored in a secure place, preferably out of sight.

3. If a mobile device is lost or stolen, promptly report the incident to the Information Technology (IT) Department and proper authorities. Also, be sure to document the serial number of your device now, for reporting purposes, in the event that it is lost or stolen.

4. Sensitive or confidential documents, if stored on the device, should be encrypted if possible.

5. Sensitive and confidential information should be removed from the mobile device before it is returned, exchanged or disposed.

6. Whenever possible all mobile devices should enable screen locking and screen timeout functions.

7. No personal information (as defined by the IT Department) shall be stored on mobile devices unless it is encrypted and permission is granted from the data owner.

8. Before a mobile device is connected to Town of Nantucket IT systems, it shall be scanned for viruses (the user risks having files on the device deleted if any viruses are detected). If media mobile device is used for transitional storage (for example copying data between systems), the data shall be securely deleted from the mobile device immediately upon completion.

Enforcement:

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

Definitions:

Mobile Devices: These include, but are not limited to, Portable Digital Assistants (PDAs), notebook computers, Tablet PCs, Palm Pilots, Microsoft Pocket PCs, RIM Blackberries, MP3 players, text pagers, smart phones, compact discs, DVD discs, memory sticks, USB drives, floppy discs and other similar devices.

User - Anyone with authorized access to Town of Nantucket information systems, including permanent and temporary employees or third-party personnel such as contractors, consultants, and other parties with valid accounts.

Roles and Responsibilities

Overview:
To define the roles and responsibilities of the Nantucket community who are responsible for information assets and security within the Town of Nantucket.

Purpose:

Information assets of the Town of Nantucket, in all its forms and throughout its life cycle, will be protected through information management policies and actions that meet applicable federal, state, regulatory, and/or contractual requirements.

Scope:

The Town of Nantucket Information Technology (IT) Department is responsible for implementing a comprehensive enterprise information security program. This responsibility is delegated to the following groups and individuals:

Management Level Roles: Information Technology Security Officer(s)

Unit Level Roles:	Department Head
	Department IT Security Liaison
	Data Steward
	Authorized User(s)

Information Technology Security Officer

The official(s) responsible for directing implementation of the enterprise information security program. The Information Technology Security Officer will:

1. Coordinate the development and maintenance of information security policies and standards.
2. Investigate security incidents and coordinate their resolution.
3. Assist Department Heads in assessing their data for classification as and advise them of available controls.
4. Implement an information security awareness program.
5. Provide consulting services for information security throughout the enterprise.
6. Maintain integrity of town office servers.
7. Enforce information security policies.

Department Heads

The senior official within a town department accountable for managing information assets. The Department Head will:

1. Approve business use of information.
2. Ensure implementation of policies, and documentation of process and procedures for guaranteeing availability of systems.
3. Determine security classification of each segment of data in partnership with the IT department.
4. Define departmental access roles and assign access for individuals based on their need to know.
5. Ensure that all department personnel with access to information assets are trained in relevant security and confidentiality policies and procedures.
6. Ensure the protection of health information assets under his/her control, including:
    - Require the completion of an information sharing agreement before access to health information assets is granted to external entities.

Department IT Security Liaison

The individual within a department who acts as a liaison for timely and relevant information flow between central networking and computer security personnel and the department. The Security Liaison will:

1. Receive all security vulnerability reports for departmental computer systems and disseminate such information to appropriate technical staff for resolution.
2. Receive network alerts, outage notifications, or other networking issues affecting the department/unit and disseminate such information to appropriate staff.
3. Coordinate departmental response to computer security incidents.

4. Implement a system for software change management and revision controls.
5. Maintain ongoing internal audit processes (to the extent technologically practical), which record system activity such as log-ins, file accesses, and security incidents.
6. Maintain records of those granted physical access to restricted areas (i.e., key card access lists).
7. Provide special handling and physical protection for health information assets, including:
    - Operating and maintenance personnel are given access only as necessary to perform system maintenance responsibilities. Authorized persons supervise all external personnel performing maintenance activities.

Data Steward

The Data Steward will:

1. Establish standards for business use of information.
2. Assign administrative responsibility to Department Heads.
3. Monitor compliance and periodically review violation reports.

4. Approve user access to information.

Authorized User

Individuals who have been granted access to specific information assets in the performance of their assigned duties are considered Authorized Users ("Users"). Users are limited to employees and/or third party vendors. Users will:

1. Seek access to data only through the authorization and access control process.
2. Access only that data which s/he has a need to know to carry out job responsibilities.
3. Disseminate data to others only when authorized by the Department Head.
4. Report access privileges inappropriate to job duties to the Department Head for correction.
5. Attend training in security and confidentiality policies/procedures.
6. Access to Level III data must be individually authorized by the Department Head and an annual confidentiality agreement must be acknowledged or signed by all authorized users.
7. Perform all responsibilities of Data Steward when placing departmental data on personally owned or managed devices.

Acceptable Use Policy

Overview:

Information Resources are strategic assets of the Town of Nantucket and must be treated and managed as valuable resources. The Town of Nantucket provides various computer resources to its employees for the purpose of assisting them in the performance of their job-related duties. This policy clearly documents expectations for appropriate use of the Town of Nantucket's assets. This Acceptable Use Policy in conjunction with the corresponding standards is established to achieve the following:

Purpose:

1. To establish appropriate and acceptable practices regarding the use of information resources.
2. To ensure compliance with applicable State law and other rules and regulations regarding the management of information resources.
3. To educate individuals who may use information resources with respect to their responsibilities associated with computer resource use.

Scope:

The Acceptable Use Policy affects all users on the town of Nantucket's network as maintained by the Information Security Department.

Policy:

1. The Information Technology (IT) Department of the Town of Nantucket will establish a periodic reporting requirement to measure the compliance and effectiveness of this policy.
2. The IT Department is responsible for implementing the requirements of this policy, or documenting non-compliance via the method described under exception handling.
3. Department Heads, in cooperation with the Information Technology Department, are required to train employees on policy and document issues.
4. All Town of Nantucket employees are required to read and acknowledge the reading of this policy.

Acceptable Use Requirements

1. The IT department will establish formal Standards and Processes to support the ongoing development and maintenance of the Town of Nantucket's Acceptable Use Policy.
2. Any security issues discovered will be reported to the IT department for follow-up investigation. Additional Reporting requirements can be located within the Policy Enforcement, Auditing and Reporting section of this policy.
3. Users must report any weaknesses in the Town of Nantucket's computer security to the IT Department. Weaknesses in computer security include unexpected software or system behavior, which may result in unintentional disclosure of information or exposure to security threats.
4. Users must report any incidents of possible misuse or violation of this Acceptable Use Policy.

5. Users must not attempt to access any data, documents, email correspondence, and programs contained on the Town of Nantucket's systems for which they do not have authorization.
6. Users must not share their account(s), passwords, Personal Identification Numbers (PIN), or similar information or devices used for identification and authorization purposes.
7. Users must not make unauthorized copies of copyrighted or Town of Nantucket owned software.
8. Users must not use non-standard shareware or freeware software without the appropriate approval of the IT Department.
9. Users must not purposely engage in activity that may harass, threaten or abuse others or intentionally access, create, store or transmit material which the town of Nantucket may deem to be offensive, indecent or obscene, or that is illegal according to local, state or federal law.
10. Users must not engage in activity that may degrade the performance of Information Resources; deprive an authorized user access to the Town of Nantucket's resources; obtain extra resources beyond those allocated; or circumvent the Town of Nantucket's computer security measures.
11. Users must not download, install or run security programs or utilities such as password cracking programs, packet sniffers, or port scanners that reveal or exploit weaknesses in the security of a the Town of Nantucket's computer resource unless approved by the IT Department.
12. The Town of Nantucket's Information Resources must not be used for personal benefit, political activity, unsolicited advertising, unauthorized fund raising, or for the solicitation of performance of any activity that is prohibited by any local, state or federal law.
13. Access to the Internet from the Town of Nantucket owned, home based, computers must adhere to all the policies. Employees must not allow family members or other non-employees to access nonpublic accessible the Town of Nantucket's computer systems.
14. Any security issues discovered will be reported to the IT department for follow-up investigation. Additional Reporting requirements can be located within the Policy Enforcement, Auditing and Reporting section of this policy.

Section 4 - Enforcement, Auditing, Reporting

1. Violation of this policy may result in disciplinary action that may include termination for employees and temporaries; termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers. Additionally, individuals are subject to loss of the Town of Nantucket's Information Resources access privileges, civil, and criminal prosecution. *(Note: Agencies need to be aware of the constantly changing legal framework of the environment in which they operate, and they must adapt accordingly. Appropriate legal advisors and/or human resources representatives should review the policy and all of the procedures in use for policy enforcement. Some legal/human resources believe it is not necessary to include this section because all policy is enforceable. In fact, if it is included in one, it may be detrimental to the enforcement of other policies that do not include the section.)*
2. The IT Department is responsible for the periodic auditing and reporting of compliance with this policy. The IT Department will be responsible for defining the format and frequency of

the reporting requirements and communicating those requirements, in writing, to the Town Manager.

3. Exceptions to this policy will be considered only when the requested exception is documented using the User Request Form and submitted to the IT Department for review and approval.

Data Classification Policy

Overview:

Data is information that supports the mission and operation of the Town of Nantucket. It is a vital asset and is owned by the Town. It is likely that Town data will be distributed across multiple departments and organizations of the Town, as well as entities outside of the Town. Town data is considered essential, and its quality must be ensured to comply with legal, regulatory, and administrative requirements. The prevalence of security incidents related to compromise of data is increasing every day and recently passed legislation institutes specific obligations and penalties surrounding compromise of some types of data

Purpose:

Data classification is one of the required components of thorough Information security. The purpose of this policy is to identify the appropriate classifications of data and the ongoing management of that classification. Classification of data is a critical part of data management which includes planning and implementing comprehensive and responsible information security practices. This document describes a standard data classification scheme, the required considerations for classification, risk assessment, security control requirements and data management and lifecycle requirements.

Scope:

For purposes of these standards, data is information maintained in an electronic, digital or optical format – such as hardcopy files. Data includes numbers, text, images and sounds, which are created, generated, sent, communicated, received by and/or stored on Town of Nantucket owned and supported Information Technology Resources. Data does not include hardware, platforms, software, applications or middleware.

Proper management of data requires agencies to perform periodic reviews of data and assess their classifications and controls. The controls for classified data must be commensurate with the level of identified risk, regulatory requirements and interagency agreements that may pertain to agency acquisition, use or maintenance of data.

Data Classification:

Authorization to access institutional data varies according to its sensitivity (the need for care or caution in handling). For each classification, several data handling requirements are defined to appropriately safeguard the information. It's important to understand that

overall sensitivity of institutional data encompasses not only its confidentiality (need for secrecy), but also the need for integrity and availability. The need for integrity, or trustworthiness, of institutional data should be considered and aligned with institutional risk; that is, what is the impact on the institution should the data not be trustworthy? Finally, the need for availability relates to the impact on the institution's ability to function should the data not be available for some period of time. There are three classification levels of relative sensitivity which apply to institutional data:

Level I: Low Sensitivity (General Use):

Definition: Data classified as having low sensitivity should be thought of as being for general use and is approved by the Department Head as available for routine public disclosure and use. Security at this level is the minimum required by the Town to protect the integrity and availability of this data.

Access: Access may be granted to any requester, or it is published with no restrictions. Public data is not considered sensitive. The integrity of "Public" data should be protected, and the appropriate Department Head must authorize replication or copying of the data in order to ensure it remains accurate over time. The impact on the Town of Nantucket should Level I data not be available is typically low, (inconvenient but not debilitating).

Examples: This may include, but is not limited to, data routinely distributed to the public regardless of whether the Town has received a public records request, such as: annual reports, publicly accessible web pages, maps, marketing materials and press statements.

Level II: Moderate Sensitivity (Internal Use):

Definition: Data classified as having medium sensitivity should be treated as internal, the release of which must be approved prior to dissemination outside the Town of Nantucket. Its compromise may inconvenience the Town, but is unlikely to result in a breach of confidentiality, loss of value or serious damage to integrity.

Access: Access must be requested from, and authorized by, the department head who is responsible for the data. Access to internal data may be authorized to groups of persons by their job classification or responsibilities ("role-based" access), and may also be limited by one's employing unit or affiliation. Non-Public or Internal data is moderately sensitive in nature. Often, Level II data is used for making decisions, and therefore it's important this information remain timely and accurate. The risk for negative impact on the Town of Nantucket should this information not be available when needed is typically moderate. Examples of Level II "Non-Public/Internal" data include project information,

Examples: Data in this category is not routinely distributed outside the Town of Nantucket. It may include, but is not limited to non-confidential data contained within: internal communications, minutes of meetings and internal project reports, official town records such as financial reports, human resources information, and budget information.

Level III: High Sensitivity (Confidential Use):

Definition: Data classified as having high sensitivity is considered confidential. Such data should not be copied or removed from the Town of Nantucket's operational control without authorized permission. High sensitivity data is subject to the most restricted distribution and must be protected at all times. Compromise of high sensitivity data could seriously damage the mission, safety or integrity of a department, its staff or its constituent. It is mandatory to protect data at this level to the highest possible degree as is prudent or as required by law.

Access: Access must be controlled from creation to destruction, and will be granted only to those persons affiliated with the Town of Nantucket who require such access in order to perform their job, or to those individuals permitted by law. Access to confidential/restricted/personal data must be individually requested and then authorized by the Department Head who is responsible for the data. Level III data is highly sensitive and may have personal privacy considerations, or may be restricted by federal or state law. In addition, the negative impact on the institution should this data be incorrect, improperly disclosed, or not available when needed is typically very high.

Examples: High Sensitivity data may include, but is not limited to, personally identifiable, legally mandated, or sensitive data associated with: investigations, bids prior to award, personnel files, trade secrets, appraisals of real property, constituent records, health records, social security and credit card numbers, contracts during negotiation and risk or vulnerability assessments.

Personally Identifiable Information shall be defined as:

- Social Security Numbers
- Medical Records
- Tax Records
- Financial/Credit Card account Numbers
- License Numbers

Data Access Policy:

- Town of Nantucket data must be protected from unauthorized modification, destruction, or disclosure. Permission to access town data will be granted to all eligible employees for legitimate town purposes.

- Authorization for access to Level II and Level III data comes from the Business Owner, and is typically made in conjunction with an acknowledgement or authorization from the requestor's department head, supervisor, or other authority.

- Where access to Level II and Level III institutional data has been authorized, use of such data shall be limited to the purpose for which access to the data was granted.

- All employees must report instances in which town data is at risk of unauthorized modification, disclosure, or destruction.

- Department Heads must ensure that all decisions regarding the collection and use of town data are in compliance with the law and with Town of Nantucket policy and procedure.

- Department Heads must ensure that appropriate security practices, consistent with the data handling requirements in this policy, are used to protect data.

- Users will respect the confidentiality and privacy of individuals whose records they access, observe ethical restrictions that apply to the information they access, and abide by applicable laws and policies with respect to accessing, using, or disclosing information.

Suggested Data Handling Requirements

	LEVEL I Low Sensitivity (Public Data)	LEVEL II Moderate Sensitivity (Non-Public/Internal Data)	LEVEL III High Sensitivity (Confidential/Restricted Data)
Mailing & Labels on Printed Reports	None	May be sent via Campus Mail; No labels required	Must be sent via Confidential envelope; Reports must be marked "Confidential"
Electronic Access	No controls	Role-based authorization	Individually authorized, with a confidentiality agreement
Secondary Use	As authorized by Business Owner	As authorized by Business Owner	Prohibited
Physical Data/Media Storage	No special controls	Access Controlled area	Access controlled and monitored area
External Data Sharing	No special controls	As allowed by Iowa Open Records Law, FERPA restrictions; or Non-UI project/study participants	As allowed by Federal regulations; Iowa Open Records Law; FERPA restrictions; and Business Associate Agreement (for PHI);
Electronic Communication	No special controls	Encryption recommended for external transmission	Encryption required for external transmission
Data Tracking	None	None	Social Security Numbers, Credit Cards, and PHI locations must be registered
Data Disposal	No controls	Recycle reports; Wipe/erase media	Shred reports; DOD-Level Wipe or destruction of electronic media
Auditing	No controls	Logins	Logins, accesses and changes
Mobile Devices	Password protection recommended; Locked when not in use	Password protected; Locked when not in use	Password protected; Locked when not in use; Encryption used for the Level III data

Definitions:

Mailing & Labels on Printed Reports – A requirement for the heading on a printed report to contain a label indicating that the information is confidential, and/or a cover page indicating the information is confidential is affixed to reports.
Electronic Access – How authorizations to information in each classification are granted.
Secondary Use – Indicates whether an authorized user of the information may repurpose the information for another reason or for a new application.
Physical Data/Media Storage – The protections required for storage of physical media that contains the information. This includes, but is not limited to workstations, servers, CD/DVD, tape, USB Flash, laptops, and PDA's.
External Data Sharing – Restrictions on appropriate sharing of the information outside of the University of Iowa
Electronic Communication – Requirements for the protection of data as transmitted over telecommunications networks.
Data Tracking – Requirements to centrally report the location (storage and use) of information with particular privacy considerations.
Data Disposal - Requirements for the proper destruction or erasure of information when decommissioned (transfer or surplus), as outlined in the University's Computer Data and Media Disposal Policy.
Auditing – Requirements for recording and preserving information accesses and/or changes, and who makes them.
Mobile Devices – Requirements for the protection of information stored locally on mobile devices. This includes, but is not limited to laptops, tablet computers, PDA's, cell phones, and USB flash drives.