#### 

IT Strategic Solutions – MMT2 Task 3

John Deardurff

Western Governors University

Table of Contents

[A. Evaluate Security Policies Regarding Ethical Issues 4](#_Toc513471302)

[A1. Unethical Uses: Internal 5](#_Toc513471303)

[1. Use of email to send PII 5](#_Toc513471304)

[2. Reading of “Personal” email 5](#_Toc513471305)

[A2. Unethical Uses: External 6](#_Toc513471306)

[1. Unencrypted Sections of Website 6](#_Toc513471307)

[2. Improper use of Cookies 6](#_Toc513471308)

[B. Evaluate Security Policies Regarding Security Threats 6](#_Toc513471309)

[Employer Security Policy 7](#_Toc513471310)

[Data Protection Policy 7](#_Toc513471311)

[Accounting Security Policy 7](#_Toc513471312)

[B1. Security Threats: Internal 7](#_Toc513471313)

[1. Lack of Storage Encryption 7](#_Toc513471314)

[2. Complicated Permission Levels 8](#_Toc513471315)

[B2. Security Threats: External 8](#_Toc513471316)

[1. Unsecured Wireless Devices 8](#_Toc513471317)

[2. Usage of IMAP for receiving email 8](#_Toc513471318)

[C. Create Updated Company Policies 9](#_Toc513471319)

[C1. Mitigate Unethical Uses 10](#_Toc513471320)

[1. Unethical - Internal: Use of email to send PII 10](#_Toc513471321)

[2. Unethical - Internal: Reading of Personal Email 10](#_Toc513471322)

[3. Unethical - External: Unencrypted Sections of Website 11](#_Toc513471323)

[4. Unethical - External: Improper Use of Cookies 11](#_Toc513471324)

[C2. Mitigate Security Threats 11](#_Toc513471325)

[1. Security Threats - Internal: Lack of Storage Encryption 11](#_Toc513471326)

[2. Security Threats - Internal: Complicated Permission Levels 11](#_Toc513471327)

[3. Security Threats - External: Unsecured Wireless Devices 11](#_Toc513471328)

[4. Security Threats - External: Usage of IMAP for Email 12](#_Toc513471329)

[D. Sources 12](#_Toc513471330)

# Evaluate Security Policies Regarding Ethical Issues

In reviewing the company’s security policies, it was revealed that the company is practicing security procedures using access control, trend analysis, system monitoring, and strong passwords. Additionally, three separate security policies have been made available to all employees upon initial hiring. The security policies are used during preliminary training to explicitly define the organizations processes, procedures, and security safeguards. During the initial training these policies must be signed and acknowledge by each new employee. The training experience also ensures that while the policies are comprehensive, they are fully explained to each employee. As the policies are updated, it is necessary to make sure that the policies are made readily accessible for each employee to review.

In reviewing the ethical aspects of the security policies a few key points were discovered. First, only the data security policy requires an employee signature. To ensure understanding and compliance with all the security policies, it should be a requirement for all employees to sign each policy. Secondary, it is important to note the difference between a policy being legal and the policy being ethical. A case in point is the monitoring of email. While any email is technically owned by the company, regardless of whether it is company related or of a personal nature, is it ethical to screen email? Being an Exchange administrator myself, I know that email can be screened and filtered without having to put “personal” in the subject line. In addition, this seems to be an ineffective way of screening email and protecting the confidentiality of trade secrets. Another area of concern in relation to email is that a procedure is not currently in place to protect the data leakage of Personally Identifiable Information (PII) from being transmitted externally from a company employee. Not only is this not keeping up with widely accepted industry standards, it is unethical to not ensure that customer and employee information is secured. While on the topic of Personally Identifiable Information (PII), it is comforting that the company says it does not rent, sale or otherwise distribute the data collected on its websites to other organizations or individuals. However, by not requiring SSL connections for all activity on all areas of the website they are passing the responsibility of security to the end user. This is not only a security issue, but unethical to imply that information provided on the website is secure when in fact that may not be the case.

## A1. Unethical Uses: Internal

### Use of email to send PII

There are not any safeguards in place to protect from an employee sending an email that contains Personally Identifiable Information (PII) that has been collected from the company. While the email system is being monitored, an unethical user could just mark the email “Personal” to skip through the monitoring process. To resolve this problem, many email systems like Exchange have a process to implement Data Protection or Transport rules to filter email that has the value fingerprints of PII such as credit card numbers or Social Security Numbers.

### Reading of “Personal” email

This relates to the same issue of having emails marked as “Personal” during the monitoring process. Relying on an email administrator to filter and monitor messages not only introduces human error, but human curiosity. While there does need to be a level of trust with employees, especially those in IT, not everyone is perfect. The mere fact someone would write “Personal” on an email would incite interest from an unethical email administrator, especially if they had a personal relationship with the employee sending the email. As mentioned previously, the monitor of email messages could be automated on the email server by using Data Protection and Transport Rules.

## A2. Unethical Uses: External

### Unencrypted Sections of Website

While efforts are made by the company to secure data transmissions by using SSL to encrypt traffic from the website, it is not currently a requirement. This leaves data transmitted across the internet susceptible to man-in-the-middle attacks by external, malicious, and unethical forces. Additionally, the public portions of the website are not monitored for the sharing of personal information. This leave customers susceptible to social engineering attacks. To solve these issues, SSL should be required for all data transmissions and all forums should be properly monitored.

### Improper use of Cookies

The company is using cookies to store information to external user’s hard drives. External unethical forces could hijack these cookies to steal Personably Identifiable Information or perform cookie replay and session hijacking attacks. The company needs to redesign the website to avoid using cookies to store information and investigate a claims-based authentication approach to secure website access.

# Evaluate Security Policies Regarding Security Threats

In reviewing the effectiveness of the company’s security policies regarding security threats it was found that A-Energy does an admirable job in their security approach. While improvements can be made, it is important to identify what the company is doing correctly. First the company has three distinct polices in place for Employer Security, Data Security, and Security Accounting.

### Employer Security Policy

The first step in any security policy is training and agreement. This policy provides that each employee is responsible for the security of their accounts and passwords. Computer security is enforced through auditing and monitoring of workstations, strong password and account lockout policies, and blocking of potential malicious websites. Physical security is implemented through high-definition security monitors of staff and guest activity.

### Data Protection Policy

The intent of this policy is to define the importance of securing data and the specific types of data classifications. Reinforcement of the responsibility and understanding of the policy is provided by having the employee sign the Data Protection Policy.

### Accounting Security Policy

Again, this policy is provided to employees at the time of acceptance of employment. Security policies are useless without adequate accounting and auditing procedures. This policy specifically outlines how collecting accounting information is used for the purpose of auditing, billing, cost allocation, and trend analysis.

## B1. Security Threats: Internal

### Lack of Storage Encryption

According to the security policy only laptops have encrypted drives. However, desktops and servers that will be using a combination of internal and external drive storage do not have any type of file level encryption which could lead to unauthorized access to data or data leakage of confidential company data. This could be solved by using Encryption File Services (EFS) to encrypt individual files and folders. For external drive encryption, BitLocker could be used to prevent loss of data, especially in the case of a lost or stolen external drive.

### Complicated Permission Levels

Managing file permissions at the individual employee level is overly complicated and difficult to manage. This could lead to employees possibly access confidential data. A simplified solution for managing document security would be to use a group-based strategy, Additionally, using newer server operating systems would allow the company to use Dynamic Access Control (DAC) which use a claims-based approach to provide access based off attributes and claim rules.

## B2. Security Threats: External

### Unsecured Wireless Devices

Each wireless connection is using MAC address filtering that does provide a level of security for Wi-Fi access. However, using WPA encryption is enabling false security. A simple internet search will describe instructions to any hacker on attack methods to compromise the wireless access points. A better solution would be to incorporate the 802.1x standard on the wireless access points to force employees to authenticate before gaining access to the network and then using an IPSec solution to encrypt the network traffic.

### Usage of IMAP for receiving email

To properly secure an email server from being compromised as a spam server, it is important to only use SMTP for sending and receiving messages. The A-Energy company is currently using IMAP on their email systems which leads to needing to provide an SMTP relay solution. Additionally, the company would be able to close both ports 143 and 993 on their firewalls once IMAP had been removed from the environment, thus providing a reduced surface area of attack. I would also suggest identifying if the email server has the POP3 service running and turn it off as well, thereby being able to close ports 110 and 995 on the firewalls.

# Create Updated Company Policies

After performing a SWOT analysis and evaluating the security policies of the A-Energy corporation, I have identified some key areas that can be used to further mitigate security concerns and ethical issues. The suggestions to update the company’s policies are as follows:

1. Require each employee to sign each of the three security policies during training to provide document proof of understanding of company policies and acknowledgement that training had been provided to the employee.
2. I would eliminate the use of including the word “Personal” in emails and restrict the use of company email for personal use.
3. I would incorporate Data Protection and Transport Rules on the email server to scan documents that are of personal nature.
4. I would incorporate Data Protection and Transport Rules on the email server to scan and filter for confidential company data as well as Personally Identifiable Information.
5. I would include a new Ethics in Security policy as a fourth document that would be required to be signed by each employee during training.
6. I would institute that all website communications must only use secure SSL connections.
7. I would institute that public forums be moderated to protect the loss of confidential or PII data to be unintentionally shared, as well as, to monitor for social engineering attacks.
8. I would instruct developers to find other solutions for the corporate website that did not use cookies. Additionally, I would look in to a solution that provided a claims-based authentication method to further secure the website.
9. I would incorporate a policy that would enforce the use of Encryption File Services for Files and Folders on internal drives and BitLocker Encryption for any external drives.
10. I would upgrade the servers to use Dynamic Access Control for file and folder access.
11. I would remove WPA from the Wi-Fi devices and incorporate 802.1x authentication with IPSec encryption.
12. I would remove IMAP and POP3 from the email server and close the appropriate ports on the firewalls to reduce the surface area of attack.

## C1. Mitigate Unethical Uses

### Unethical - Internal: Use of email to send PII

The updated company policies that would be used to mitigate this unethical use would be: 1. By requiring each employee to sign of the policies during training they are accountable for security. 2. Eliminating the use of the word “Personal” in emails and restricting the use of company email for personal use mitigate the possibility of improper usage of company email. 3. Incorporating Data Protection and Transport Rules would automate the scanning of email. 4. Using Data Protection and Transport Rules will filter for PII data. 5. Including a fourth signed document specific to ethics would raise awareness for the employees.

### Unethical - Internal: Reading of Personal Email

The same policies as previously mentioned would also apply to this internal unethical dilemma. Specifically, removing the usage of the word “Personal” from emails, restricting the use of personal email, and automating the filter and monitor of email by using Data Protections and Transport rules, not only mitigates, but eliminates the process of email administrators from access these emails.

### Unethical - External: Unencrypted Sections of Website

This external unethical issue is mitigated by requiring all data transmissions to use SSL connections. In addition, public forums would me monitored for social engineering attacks.

### Unethical - External: Improper Use of Cookies

Instructing developers to use more secure methods of authenticating and storing data, the suggested policy updates eliminates the potential of unethical external people from performing cross-site attacks and potentially hijacking customer information.

## C2. Mitigate Security Threats

### Security Threats - Internal: Lack of Storage Encryption

The suggested policy updates to require EFS for files and folders and BitLocker for External Drives would ensure that data was encrypted and less susceptible to data loss and data leakage.

### Security Threats - Internal: Complicated Permission Levels

The suggested policy update to upgrade servers to support Dynamic Access Control for file and folder access would simplify access to company documents while providing a more dynamic and secure solution.

### Security Threats - External: Unsecured Wireless Devices

By removing WPA and then incorporating 802.1x authentication and IPSec encryption, this suggestion policy increases the security of data in transit while forcing only authorized users access to the corporate network.

### Security Threats - External: Usage of IMAP for Email

This suggested company policy of removing IMAP and POP3 from the email servers not only mitigates the possibility of malicious users from using the company messaging system for spam attacks, it also reduces the surface area of attack for the network by being able to close four ports on all the firewalls.

# Sources

No sources were used in the writing of this report.