Email Policy for [COMPANY NAME]

Josiah Baker

Liberty University

CSIS340: Studies in Information Security (D01)

April 17, 2023

DISCLAIMER

Within this sample email policy are several references to other policies, such as an Acceptable Use Policy (AUP). These are fictional policies that do not exist and are assumed to already exist within an organization’s system. I use them within the paper since a lot of policies work together.

Email Policy for [COMPANY NAME]

Overview

Emails are the most prevalent form of communication within [COMPANY NAME]. Because of this, [COMPANY NAME] will be implementing an Email use policy to inform employees what they are allowed to use their emails for, as well as what to be concerned about regarding security.

First consideration is the threats emails impose on a system's security. Back in 2019, Mimecast did a study on the frequency an email contains a malicious URL and found some very startling results. In the study of 28,407,664 emails, 463,546 of them were falsely marked as secure (gale.com, 2019). They also found that in another study of 232,010,981 emails about 25,000,000 were spam, 26,000 had malware attachments, 53,000 were impersonation attacks, and 24,000 were dangerous file types (gale.com, 2019). These emails were not detected by any security system and made their way into employee inboxes.

The contents within the email can often be malicious and even inappropriate. In 2001, a worker for Dell in France accidentally sent inappropriate content to a manager in the U.S. (Kelleher, 2005). This action resulted in the immediate termination of the employee, as well as a damaged reputation.

From these examples we can see that how an email is used can have serious implications for each employee and the company.

Purpose

This email policy aims to inform employees of what is acceptable behavior regarding their company given email, as well as protocol to follow when receiving unknown emails. This is to protect the employees of [COMPANY NAME]. It is also meant to reduce the cyber threats [COMPANY NAME] has to handle.

Scope

According to isms.online, something that needs to be considered is what part, or who, in a business will need to use information or technological assets that are valuable. It has already been established that security risk can come through an email. Since all employees have a company email, the scope of this policy is all employees. Nobody is exempt, since it is important that the whole organization works in unison to ensure the security of [COMPANY NAME].

Policy

First, all emails must abide by the ethical policy document, and be safe and harmless in the workplace. They must also adhere to the Acceptable Use Policy (AUP). Furthermore, emails should not be used for anything outside of business. The company email has been created for you by the company, and, therefore, should be used exclusively for business related purposes (SANS, 2013). Emailing personal contacts as well as subscribing to any service that is not being used for business purposes are prohibited.

An email that contains any attachment or URLs should be scanned with the company provided malware scanner. This ensures the email received does not contain malicious code.

Any email received that does pertain to business matters must be filed and saved in a matter that can be retrieved easily in the future. Deleting company emails is strictly prohibited. Company emails should also stay strictly within the business. Email makes it easy to forward information to other, third-party sources (SANS, 2013). Emails can only be sent within the company unless specific permission has been granted.

According to the Electronic Communications Privacy Act (ECPA), [COMPANY NAME] can monitor all employee emails (ojp.gov). Legally, [COMPANY NAME] can review employee emails, which means each employee should take caution in their email use, knowing it may be viewed by another employee within [COMPANY NAME].

Policy Compliance

Violation of any of the policies may have serious consequences. One result could be the employee being immediately terminated from their position within [COMPANY NAME]. According to Corey A. Ciocchetti in "The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring", just over a quarter of employers who monitor employee emails have terminated at least one employee due to the nature of the email (wiley.com). Sixty-four percent of these terminations were because the employee violated one of the email policies. As previously stated, [COMPANY NAME] has the right to monitor emails and will take appropriate action if any of the policies is not adhered to.

Exceptions to the stated policies are possible, but unlikely. To receive an exception from one of the stated policies, please contact one of the cybersecurity team members (SANS, 2013).

Related Standards

One area heavily covered in this policy is what is considered appropriate or not appropriate regarding use of the company email. One aspect to take into consideration is what should be deemed ethical or moral. As previously stated, violation of the email policy may result in termination from [COMPANY NAME]. However, each employee should feel ethically obligated to adhere to the email policies (Ruighaver, 2010). By adhering to the policies, an employee's reputation amongst other employees and supervisors will increase and could result in a possible promotion. However, the employee must prove to be trustworthy, as well as being an ethical decision maker. For further information regarding what is ethical within [COMPANY NAME], please refer to the Ethics Policy document.

Definitions

AUP (Acceptable Use Policy) – defines what is appropriate use of company computers and networks, as well as the consequences of terminating the AUP policy (Johnson, 2022).

Breach – "The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrent where: a person other than an authorized user access or potentially accesses personally identifiable information; or an authorized user accesses personally identifiable information for another authorized purpose." (nist.gov)

Terms

The threat of a breach and security issue is always present. [COMPANY NAME] has created this document to allow employees to be prepared for the threats that are present, as well as be aware of the actions [COMPANY NAME] can take regarding email monitoring. Eric Mankwa says in "Establishing Information Security Policy Compliance Culture in Organizations" that the weakest point in a company, regardless of any policy or elaborate security system, is ultimately the people that work there. The security of the entire system is dependent on the individual person. That is why it is critical for [COMPANY NAME] and all the employees to work in a unified fashion, effectively pursuing security, and wellness of the company. By encouraging each other and working together, [COMPANY NAME] can remain a secure, safe place for all the employees.

Summary

There are many threats that are posed using emails. Whether that be personal liability for the content an employee puts within these emails, or the security risks associated with malicious email. However, these risks can be avoided. By adhering to this email framework, each employee can protect [COMPANY NAME].

References

Amankwa, E., Loock, M., & Kritzinger, E. (2018). Establishing information security policy compliance culture in organizations. *Information and Computer Security, 26*(4), 420-436. https://doi.org/10.1108/ICS-09-2017-0063

Breach. NIST. (n.d.). Retrieved April 17, 2023, from https://csrc.nist.gov/glossary/term/breach

Ciocchetti, C.A. (2011), The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring. American Business Law Journal, 48: 285-369. https://doi.org/10.1111/j.1744-1714.2011.01116.x

Determining the scope of the ISMS – ISO 27001 requirement 4.3. ISMS.online. (n.d.). Retrieved April 17, 2023 from https://www.isms.online/iso-27001/determining-scopeinformationsecurity-management-system/

Johnson, R., & Easttom, C. (2022). *Security policies and implementation issues*. Jones & Bartlett Learning.

Kelleher, Z., & Hall, H. (2005). Response to risk: Experts and end-user perspectives on email security, and the role of the business information professional in policy development. Business Information Review, 22(1), 46–52. https://doi.org/10.1177/0266382105052266

Mimecast Highlights Results of Email Security Risk Assessment Report. (2019, March 10). *Entertainment Close-up*. https://link.gale.com/apps/doc/A577776462/BIC?u=vic_liberty&sid=summon&xid=2e0b7781

Ruighaver, A. B., Maynard, S. B., & Warren, M. (2010, October). *Ethical Decision Making: Improving the Quality of Acceptable Use Policies*. ScienceDirect. Retrieved April 17, 2023, from https://doi.org/10.1016/j.cose.2010.05.004

Security policy templates. SANS Institute. (2013). Retrieved April 17, 2023, from https://www.sans.org/information-security-policy/