INFORMATION SECURITY POLICIES:

Five Important Policies Needed

Jasmyn Wilhelm

Department of Cybersecurity, Old Dominion University

CYSE 300: Introduction to Cybersecurity

Malik A. Gladden

17 September 2023

A policy is a rule or a plan in place for making decisions whether in security or business. It can be defined as a procedure or a plan of action to guide in any situation. Trainees at a new company have plans and policies already in place that need to be followed in how business takes place and what not to do. This is the same definition for security just with a different type of data. Instead of in sales by not following procedure you can lose a customer you can in security cause a massive data breach.

One of the most important items to include in a security policy is training. Cybersecurity training can be a major key in what not to do or can be defined as a cybersecurity incident such as spillage. All government employees are required to complete training whether online or in person once a year or their access is revoked. This can go hand in hand with an acceptable use policy on what can and cannot be done with data, hardware, and critical information. Leaving a laptop out in public that is either government or company equipment is against the acceptable use policy and is a cybersecurity incident especially if it contains confidential information.

To counteract a violation in either the acceptable use policy or security policy an incident response policy should be in place in how to respond to the different types of risks associated with the violation. This policy should be given to all employees to give directions on how to respond, prepare, identify, and recover from such actions. Information on who to report to and the chain of command as you could say should be listed so the information is relayed as soon as possible and before the incident can become bigger.

One policy that is not used by every organization but is just as important is a BYOD or Bring Your Own Device policy. This policy can cover what outside devices can be brought and what sites or data may be taken or accessed. This policy can vary from each organization, but it can detail what technology can be used or brought, how it is allowed to be used, and what guidelines must be followed. This type of policy is somewhat different from the others as it explains how to use other equipment provided and

what is provided. Meanwhile, this policy protects what is brought into the company and can limit what leaves the premises. This still can allow employees to have what devices they value most and can prevent companies from buying the items out of pocket.

In today's age with the type of technology and convenience available, a lot of companies allow others to use remote access to do their work from home, especially since 2020 when the Coronavirus was world spread. While this was nice for employees and did show an increase in productivity this does cause security risks. Remote access allows the employee to connect to the company network to access the files they need to use kept on the servers. This policy can define what can be sent and received and who exactly is allowed to access the devices or servers. This can be similar to onsite policies but can require stronger encryptions, refraining from connecting to an unauthorized internet connection at the same time as accessing the server, and so on.

The three core objectives to keep in mind when creating these policies are confidentiality, integrity, and availability. The explanation of these policies may vary by company, but the best practice is to include as much detail as possible and include charts and tables to help guide and show the flow of the procedure. Consequences should be listed for not following policy and exactly what type of offense it can entail. Detail and well-written explanations are key for these types of documents and rules. Making sure all employees understand all the policies and definitions will be a key factor for customer and consumer safety.

References

Adsero Security. (2023, August 23). *10 must have IT security policies for every organization*. https://www.adserosecurity.com/security-learning-center/ten-it-security-policies-every-organization-should-have/

Bourgeois, D. T. (2014, February). *Information systems for business and beyond - saylor academy*. Saylor. https://resources.saylor.org/wwwresources/archived/site/textbooks/Information%20Systems%20for%20Business%20and%20Beyond.pdf

Chouffani, R., & Wigmore, I. (2021, May 20). *What is BYOD? bring your own device definition*. WhatIs.com. https://www.techtarget.com/whatis/definition/BYOD-bring-your-own-device#:~:text=BYOD%20(bring%20your%20own%20device)%20is%20a%20policy%20that%20allows,accessing%20corporate%20apps%20and%20data.

Uniserve Hong Kong Ltd. (n.d.). *Security policies your organization should have*. Uniserve IT Solutions. https://uniserveit.com/blog/security-policies-your-organization-should-have