Clean Desk Policy for H.E. Games LLC.

Hayden Eubanks

Liberty University

Studies in Information Security, CSIS 340

March 31, 2022

Clean Desk Policy for H.E. Games LLC.

Overview

Having a clean desk policy in place can increase the security of data in a workplace tremendously by ensuring both physical and digital access to data is locked away while the user is not at the workstation (Masilela & Nel, 2021). Human error is among the top reasons that data breaches occur in a workplace (Ayo et al., 2018) and cybercriminals exploit human fallibility as one of the primary vectors of attack (Jayatilaka et al., 2021). By employing a good clean desk policy, employees can transition from being a weakness in information security to being an asset to the defense of information (Jayatilaka et al., 2021). The standards outlined in the clean desk policy for H.E. Games LLC concern the expectations of employees to handle access to data in a way that ensures its confidentiality when the employee is not present with the data (Jayatilaka et al., 2021). Adherence to the clean desk policy not only ensures data confidentiality but also the integrity of data as the answers to whether the data has been modified and who has modified the data can be known to a greater degree of certainty (Johnson & Easttom, 2020). Having a clean desk policy in place can increase employee awareness toward the security of data while they are not present (Johnson & Easttom, 2020) as well as cultivate a workplace culture in which information security accountability is upheld among employees (Alotaibi et al., 2019). Babapour Chafi and Rolfö (2019) affirmed this through their research and stated that positive implementation of a clean desk policy in a workplace environment can create a culture where employees practice clean desk security principles and mutual accountability is obtained within the office ecosystem.

Purpose

The primary purpose of the clean desk policy at H.E. Games LLC is to increase information security and therefore protect the intellectual property of the company. Mishra et al. (2022) stated that having cybersecurity policies for the appropriate handling of company information is essential and equal in value to implementing cyber-security systems. Implementing a clean desk policy will utilize controls found in ISO/IEC 27002 (International Organization for Standardization, 2013) to protect the intellectual property of H.E. Games and outline a standard for what employees must accomplish to achieve compliance with the clean desk policy.

General Objective

H.E. Games LLC derives a large portion of the company's value from its intellectual property and upcoming projects. Because of this, H.E. Games LLC has put a high value on the protection of their intellectual property, and implementing a clean desk policy is a means to accomplish that protection. By increasing data protection through policies such as the clean desk policy, H.E. Games LLC can better maintain control of information releases and advertising campaigns involving their intellectual property as well as increase protection from damages incurred from the negative public image associated with a data leak (Johnson & Easttom, 2020).

Protocol

If an employee notices a breach of the protocol outlined in this policy, they are to first secure the data by locking the computer or papers away (Jayatilaka et al., 2021) and then immediately alert a member of management and fill out an incident report on the company’s online incident report portal. In the case that the egregious party is the reporter’s acting manager, the incident can be reported to the human resources department by email at humanresources@HEGames.co.uk or by phone at +44 5555-555555. If a failure of compliance is

reported, the severity of the incident will be assessed by the employee at fault's manager and a corrective action plan will be put into effect in conjunction with the human resources department.

Scope

The clean desk policy for H.E. Games LLC applies to all data and intellectual property, physical or electronic, owned by H.E. Games. Further, this policy applies to the accessing of data on devices belonging to H.E. Games as well as all other devices company data may be accessed from. All employees of H.E. Games interacting with company data must be compliant with the clean desk policy as outlined and failure to be compliant will result in corrective action.

Policy Compliance

When devices or documents containing information belonging to H.E. Games LLC are left unattended, the data must be fully secured to not allow outside access (Alotaibi et al., 2019). Securing data can be accomplished by locking documents in a desk or briefcase requiring a combination or key to open (Alotaibi et al., 2019) or locking a computer that requires two-factor authentication to open and at least one of the factors must be a password (Mishra et al., 2022). Passwords, combinations, or keys used to access data are considered sensitive information and fall under the scope of this policy meaning that they cannot be left at a workstation and must be secured in the same manner as other sensitive information (Alotaibi et al., 2019). Data left unattended for more than fifteen minutes within the office spaces of H.E. Games LLC or more than three minutes outside of the office spaces shall be in breach of this policy and subjectable to action.

Weekly walkthrough spot testing conducted by managers (Masilela & Nel, 2021) as well as annual in-person penetration testing conducted by an outsourced company (Jayatilaka et al.,

2021) shall be conducted to ensure compliance is being held by employees. A breach of the policy outlined herein shall be reviewed by the employee at fault's manager and human resources department and corrective action shall be taken concerning the severity and frequency of the offending act (Alotaibi et al., 2019). All exceptions to this policy must be approved by the manager in charge of overseeing the employee before the sensitive data is left unattended.

Findings

Human error is the primary cause of fault in cases where data confidentiality is breached (Alotaibi et al., 2019). Alotaibi et al. (2019) then furthered this claim in their research where they stated that human error is unpredictable as it is often spontaneous and therefore difficult to defend against. By enforcing a clean desk policy, human error can be reduced as employee awareness is raised and a culture of protecting data while not in use is developed (Jayatilaka et al., 2021). The social pressure toward compliance that comes with a culture of protecting information can be a factor in transforming employees into a layer of data security (Jayatilaka et al., 2021). Babapour Chafi & Rolfö (2019) found in their research that employing a clean desk policy not only improved information security but also improved company efficiency as workstations were more accessible and able to be used when needed as they were not occupied by sensitive information.

Related Standards

Physical Security

Full compliance with a clean desk policy can be subverted by a lack of well-maintained physical security in the offices of H.E. Games LLC and the infrastructure in which data is stored. H.E. Games LLC will therefore ensure all locks to storage areas of sensitive information exceed the minimum-security standard determined by H.E. Games' Chief Security Officer. H.E. Games

will also ensure all sensitive data storage locations including servers, filing cabinets, and desks shall remain in rooms with locks on the doors which meet the same security standard outlined above.

Awareness Training

Employee error is often the result of a breach of data (Walker-Roberts et al., 2020) with clean desk violations being an example and a large portion of employee error is committed because of a lack of awareness of security threats and prevention methods (Singh & Singh, 2017). By seeking to educate employees on the principles behind the clean desk policy and the threats that exist to intellectual property in the workplace, H.E. Games LLC can better protect their intellectual property by simultaneously removing a vulnerability and implementing a layer of security (Jayatilaka et al., 2021). This training will be given upon employee induction and then repeated annually through the online corporate data-security training platform.

Definitions

Clean desk: Clean desk concepts refer to the idea of locking away data when it is not in use, such as when papers are locked away from on a desk at the end of a workday (Johnson & Easttom, 2020). In the context of H.E. Games' clean desk policy, clean desk refers to the safe storing of all sensitive data digital or otherwise owned by the H.E. Games when it is not in use.

Data integrity: Data integrity refers to the ability to affirm that data has not been edited, or if it has been edited, knowing who has edited it and what they have changed (Johnson & Easttom, 2020).

Data confidentiality: Data confidentiality refers to the ability to keep data from being viewed by those who do not have access to it (Johnson & Easttom, 2020).

Sensitive data: Sensitive data refers to all data or intellectual property which is not given global accessibility for members inside and outside of H.E. Games.

Terms

As technical security continues to increase, malicious actors aim to exploit the vulnerabilities of human error and weak human controls to gain access to confidential data (Jayatilaka et al., 2021). H.E. Games hopes to champion its employees to a higher standard of data security as it protects confidential data in the workplace through policies such as the clean desk policy. Upon joining the company, awareness training on data protection including the clean desk policy will be given and then annually will be refreshed through the company's online training platform. These trainings are mandatory and must be completed by all employees of H.E. Games and contracted partners working with the data or intellectual property of H.E. Games LLC. Any breach of the clean desk policy must be reported to the employee's acting manager and an investigation will be undertaken by the employee and human resources department to determine a suitable corrective action plan based on the frequency and severity of the incident (Alotaibi et al., 2019). Employing good data security is essential to the operations of H.E. Games LLC and the standards outlined in this policy are an important method of protecting company data.

Summary

Poor employee decisions regarding the data and intellectual property of H.E. Games LLC can be a vulnerability to data security (Ayo et al., 2018). Enforcing the clean desk policies outlined above can contribute to minimizing that risk while increasing the security of data and ensuring physical and digital data are secured. The expectations on employees of H.E. Games LLC to handle access to data protects the confidentiality of data when the employee is not

present (Jayatilaka et al., 2021) and can thwart malicious actors from exploiting human weakness (Jayatilaka et al., 2021). Having a clean desk policy in place brings awareness to the employee of security concepts regarding the data they interact with (Johnson & Easttom, 2020) and fosters a culture in the workplace where peer accountability can be established (Alotaibi et al., 2019). By implementing these clean desk policies H.E. Games LLC can better control access to their data and intellectual property and become better protected from the damages associated with a breach of that data.

References

Alotaibi, M. J., Furnell, S., & Clarke, N. (2019). A framework for reporting and dealing with end-user security policy compliance. Information Management & Computer Security, 27(1), 2-25. https://doi.org/10.1108/ICS-12-2017-0097

Ayo, S. C., Ngala, B., Amzat, O., Khoshi, R. L., & Madusanka, S. I. (2018). Information security risks assessment: A case study. ArXiv Preprint. arXiv:1812.04659. https://arxiv.org/abs/1812.04659

Babapour Chafi, M., & Rolfö, L. (2019). Policies in activity-based flexible offices: 'I am sloppy with clean-desking. we don't really know the rules.'. Ergonomics, 62(1), 1-20. https://doi.org/10.1080/00140139.2018.1516805

International Organization for Standardization. (2013), Information technology – security techniques – code of practice for information security controls (ISO/IEC Standard No. 27002). International Organization for Standardization. www.iso.org/standard/54533.html

Jayatilaka, A., Beu, N., Baetu, I., Zahedi, M., Babar, M. A., Hartley, L., & Lewinsmith, W. (2021). Evaluation of security training and awareness programs: Review of current practices and guidelines. ArXiv Preprint. arXiv:2112.06356. https://arxiv.org/abs/2112.06356

Johnson, R., & Easttom, C. (2020). Security policies and implementation issues (3rd Edition). Jones & Bartlett Learning. https://libertyonline.vitalsource.com/books/9781284200034

Masilela, L., & Nel, D. (2021). The role of data and information security governance in protecting public sector data and information assets in national government in South

Africa. Africa's Public Service Delivery and Performance Review, 9(1), 385. https://journals.co.za/doi/full/10.4102/apsdpr.v9i1.385

Mishra, A., Alzoubi, Y. I., Gill, A. Q., & Anwar, M. J. (2022). Cybersecurity enterprises policies: A comparative study. Sensors (Basel, Switzerland), 22(2), 538. https://doi.org/10.3390/s22020538

Singh, A., & Singh, A. (2017). Review of cyber threats in social networking websites. *International Journal of Advanced Research in Computer Science, 8*(5), 2695. https://doi.org/10.26483/ijarcs.v8i5.4102

Walker-Roberts, S., Hammoudeh, M., Aldabbas, O., Aydin, M., & Dehghantanha, A. (2020). Threats on the horizon: Understanding security threats in the era of cyber-physical systems. *The Journal of Supercomputing*, 76(4), 2643-2664. https://doi.org/10.1007/s11227-019-03028-9