Acceptable Use Policy for H.E. Games LLC.

Hayden Eubanks

Liberty University

Studies in Information Security, CSIS 340

May 2, 2022

Acceptable Use Policy for H.E. Games LLC.

Overview

H.E. Games LLC aims to employ an acceptable use policy within the organization to inform employees of appropriate usage of the internet and computer resources belonging to H.E. Games (Masilela & Nel, 2021). Social engineering and human error are among the most common reasons for breaches of company information (Ayo et al., 2018), and by creating an acceptable use policy, users can be empowered to use company technology resources and the risk of company data being exposed through user error is mitigated (Robinson & McMenemy, 2021). A successfully implemented acceptable use policy can increase the efficiency and quality of an employee's work and diminish the need to apply automated censorship to websites (Robinson & McMenemy, 2020). This can therefore decrease the number of useful sites censored by automated software and further optimize the efficiency of H.E. Games' computer resources (Robinson & McMenemy, 2020). The internet and technology are essential tools in today's workplace and an acceptable use policy allows for the best use of those resources (Glen, 2021).

The acceptable use policy outlines expectations toward employees regarding internet usage, usage of company computers and technology, usage of company email, and usage of company software. These resources are to be utilized for business use only and H.E. Games LLC reserves the right to monitor usage, block material, and control the settings and usage of these resources. The controls H.E. Games has placed on technological resources in this way are not aimed to restrict and hinder employee usability, but to champion employees in their usage of company resources and give grounds for employees to report and stop inappropriate usage (Robinson & McMenemy, 2021).

Purpose

The purpose of H.E. Games LLC's acceptable use policy is to outline the acceptable and unacceptable use of the internet and technology at or belonging to H.E. Games LLC. In doing so, H.E. Games hopes to mitigate corporate risks and increase user efficiency in the workplace (Johnson & Easttom, 2020). Inappropriate usage of these company resources can create vulnerabilities in data security, waste company time and bandwidth, and enable access to content inappropriate for the workplace (Mishra et al., 2022). Having an acceptable use policy in place further enables H.E. Games LLC to shape company culture (Glen, 2021) and give language to enable employees to report the inappropriate usage of company resources (Robinson & McMenemy, 2021). H.E. Games will employ controls outlined in ISO/IEC 27002 (International Organization for Standardization, 2013) to further enable employees to abide by the acceptable use policy and monitor for misuse.

General Objective

H.E. Games recognizes that throughout the company's operations, much of the work is performed by employees using technology and the inherent value of the company lies in the employee's effective use of those resources. For this reason, H.E. Games has recognized the high value in championing employees to get the most efficient use of computer resources and enacting an acceptable use policy aims to further this goal. In implementing an acceptable use policy, H.E. Games also aims to mitigate the risks associated with intentional or accidental misuse of company resources and in doing so strengthen the security of company data (Sauers & Richardson, 2019). As the acceptable use policy is put into action, employee awareness of cyber threats can be raised and the objective of mitigating risks can be further accomplished (Mishra et al., 2022)

Protocol

If a breach of the acceptable use policy described herein is observed, the noticing employee is to immediately report the incident to the employee at fault's manager and file an incident report online at H.E. Games' incident report portal. All breaches of the acceptable use policy may be reported to human resources by email at humanResources@HEGames.co.uk or by phone at +44 1111-111111. Upon reporting, the incident severity will be assessed by the direct manager of the employee at fault and the human resources department and corrective action will be implemented.

Scope

H.E. Games' acceptable use policy applies to all data and electronic devices belonging to H.E. Games as well as access to the internet from H.E. Games' offices. This includes but is not limited to company email, computer devices, and technologies belonging to H.E. Games, all software and applications installed on company devices, the operating system and settings of employee workstations, and internet access to and from company networks (Sauers & Richardson, 2019). All employees and contractors interacting with technology resources belonging to H.E. Games must be compliant with the acceptable use policy and a failure of compliance will result in corrective action and in serious incidents termination or legal action against the egregious party. All exceptions to the acceptable use policy must receive a combined approval from an active manager above the employee requesting the exception and the human resources department.

Policy Compliance

H.E. Games LLC maintains the right to monitor usage, block material, and control the settings and usage of technological resources owned by H.E. Games. Usage of the technological property of H.E. Games must be thoroughly monitored and controlled to prevent exposure of company data or misuse of resources which could cause damage to the company (Mishra et al., 2022). H.E. Games' monitoring of company networks and devices includes but is not limited to scanning company email and email attachments, running antivirus scans on devices, logging user activity including internet usage, and logging data access (Mishra et al., 2022). H.E. Games also reserves the right to filter content such as pornographic and other explicit material which is deemed offensive or inappropriate for the workplace (Johnson & Easttom, 2020). Any other content that the human resources department also deems to be inappropriate for the workplace shall be blocked such as but not limited to gambling sites, gaming services, streaming services, and websites participating in copyright infringement or other illegal activity (Robinson & McMenemy, 2020).

Employees, contractors, and other users of H.E. Games' technological resources and data are expected to use company resources in a way that does not promote harm to H.E. Games LLC, the company's reputation, or any resources belonging to the company (Robinson & McMenemy, 2021). One way in which employees can engage with acceptable use is through the use of H.E. Games' electronic devices. When using company devices, employees are not to install software or alter the settings of company devices without the approval of the employee's active manager and the IT department (Sauers & Richardson, 2019).

Employees of H.E. Games are required to exhibit mutual respect through online communications and obscenity or language which would harm the reputation of H.E. Games is prohibited (Sauers & Richardson, 2019). Offensive content detected in company email or on the company's network will be flagged for review by the human resources department who will conduct an investigation and decide if further action should be taken. In enforcing this aspect of the acceptable use policy, H.E. Games hopes to strengthen the user's awareness of their digital citizenship and online etiquette imparting to them a valuable life skill that they can use in all their online interactions (Robinson & McMenemy, 2021).

All employees interacting with data belonging to H.E. Games must handle the data in a way that access is not given to unauthorized parties. This includes ensuring data is encrypted when it is stored or leaves the network and that sensitive data is not sent outside of the network through email or other channels (Mishra et al., 2022). Any attempt to bypass the security controls for data access or attempt to make classified data available at a lower classification level will result in an immediate investigation and corrective action from the IT and human resource departments.

Findings

In corporations such as H.E. Games, one of the primary causes of breaches to data security is human error (Ayo et al., 2018). Ayo et al. (2018) confirmed this through their research where they noted that acceptable use policies can be implemented to reduce risks associated with social engineering and intentional or accidental human error. Through acceptable use policies, the risks associated with IT systems can be reduced and the overall risk appetite of the organization can be kept at a manageable level (Ayo et al., 2018). In addition to this, having an acceptable use policy in place can increase the user's awareness of security threats and how the acceptable use policy mitigates those threats (Mishra et al., 2022). Mishra et al. (2022) highlighted the importance of user awareness generated through policy as they emphasized that user awareness can be more effective at improving data security than cybersecurity tools.

Related Standards

Data Classification

All data created on and by H.E. Games is the sole property of H.E. Games LLC and the acceptable use policy outlines the expectation for how employees can interact with that data. Data classification is closely linked to this standard as the classification of data determines who has access to it and the classification system can be bypassed by misuse from a user (Mishra et al., 2022). Data that is classed as anything other than public, cannot be sent outside of the internal network without permission from two separate managers. Technical controls are put in place to monitor access to files and file transfers to help ensure that this expectation is being met (Mishra et al., 2022). By controlling and monitoring the classification, access, and flow of data, information security can be increased, and the risk of inappropriate access mitigated.

Password Policy

Passwords can be the target of social engineering attacks (Ayo et al., 2018) and weak or unsecured passwords may leave a system and its data vulnerable to a breach (Johnson & Easttom, 2020). To be compliant with the acceptable use policy, employees must under no circumstances share their password with anyone or leave their workstation unprotected without a password. In addition to this, passwords cannot be written down and stored at a workstation and password hints on the lock screens are prohibited. Strong passwords can be rendered useless if they are easy to access (Mishra et al., 2022) so it is imperative that the acceptable use of passwords is practiced in conjunction with strong password usage.

Awareness Training

One objective of the acceptable use policy is to increase the awareness of users of potential threats and in doing so increase the security of the company’s data (Mishra et al., 2022). In attempting to educate users on the values and principles behind the acceptable use policy, H.E. Games can better protect their data and remove the vulnerability of a user’s lack of awareness of security issues (Ayo et al., 2018). Awareness training and agreement to the acceptable use policy must be completed upon employee induction and before they are given access to H.E. Games' computer systems. The awareness training will then be repeated annually, and completion will be monitored through H.E. Games' online training platform.

Definitions

Acceptable use: Acceptable use refers to the expectations of how all staff will interact with restrictions regarding the use of the company network, internet, and technologies (Masilela & Nel, 2021).

Digital citizenship: Digital citizenship refers to a user's online etiquette and how they present themselves online as a citizen of the web (Robinson & McMenemy, 2021). The implied practice of good digital citizenship involves treating others online with respect and not posting information detrimental to one's reputation (Robinson & McMenemy, 2021).

Social Engineering: Social engineering is a tactic used by malicious actors to gain the information they would otherwise not have access to through deceptive social encounters (Ayo et al., 2018).

Terms

H.E. Games aims to champion its employees to a greater degree of awareness, efficiency, and data security through the implementation of the acceptable use policy. H.E. Games LLC will instruct awareness training including the acceptable use of technology and the internet within the workplace. It is mandatory to attend these trainings and the awareness training module must be completed by all employees of H.E. Games, contractors, and other users gaining access to technology or data owned by H.E. Games. All discovered breaches of the acceptable use policy must be promptly reported to the offending employee's manager and together with the human resources department, corrective action will be taken. Data security is foundational to the success of H.E. Games and the acceptable use policy is an integral part of protecting data and therefore the company's success.

Summary

Having an effective acceptable use policy is critical to both the efficiency and security of the use of data and technology at H.E. Games (Robinson & McMenemy, 2021). Through the integration of an acceptable use policy in the workplace, the risks of human error can be mitigated (Ayo et al., 2018) and the awareness of employees of security threats can grow to turn them into valuable assets for protecting information (Robinson & McMenemy, 2021). As the internet and computer systems become more essential in the workplace, having an acceptable use policy allows the use of these valuable tools to grow (Glen, 2021) while keeping the associated risks at a manageable level (Mishra et al., 2022).

References

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

Glen, C. M. (2021). Norm entrepreneurship in global cybersecurity. *Politics & Policy (Statesboro, Ga.), 49*(5), 1121-1145. https://doi.org/10.1111/polp.12430

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

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), 1-10. 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

Robinson, E., & McMenemy, D. (2021). Communicating patron rights and responsibilities transparently: Creating a model internet acceptable use policy for UK public libraries. *Public Library Quarterly (New York, N.Y.)*, 1-25. https://doi.org/10.1080/01616846.2021.1936883

Robinson, E., & McMenemy, D. (2020). ‘To be understood as to understand’: A readability analysis of public library acceptable use policies. *Journal of Librarianship and Information Science, 52*(3), 713-725. https://doi.org/10.1177/0961000619871598

Sauers, N. J., & Richardson, J. W. (2019). Leading the pack: Developing empowering responsible use policies. *Journal of Research on Technology in Education, 51*(1), 27-42. https://doi.org/10.1080/15391523.2018.1539644