Fair and Responsible use Policy (ISSP

Keith M. Hall

College of Science and Technology, Bellevue University

CIS608-T301: Information Security Management

Professor Kayleen Amerson

September 25, 2022

Fair and Responsible use Policy (ISSP)

Purpose

This policy aims to establish and protect the availability, confidentiality, and integrity of sensitive information of family members and regulate fair use of the internet, email, social media accounts, streaming movie services, and electronic resources, including computers, fax machines, printers, scanners, and wireless routers owned by the parents of the Hall family household.

Authorized Uses

This policy applies to all members of the Hall family, their guests, and all visitors who enter the Hall family residence. All electronic resources in the residence's main living area are the sole property of the parents of the Hall family and designated for the private use of family members to conduct educational and employment-related activities. Authorized users must comply with the fair and responsible use policies that comprise the contents of this document. Any use of electronic assets for purposes not explicitly identified is considered a misuse of equipment. Electronic asset owners notify users that their online behavior may be periodically monitored.

Prohibited Uses

1. All electronic resources in the residence's main living area must remain in the living area.

2. All electronic resources are designated for the private use of family members to conduct educational and employment-related activities.

3. Privacy

a. No family member shall attempt to access another family member's email, social media, or any other account protected by username and/or password.

4. Downloading

a. Family members are confined to downloading materials, files, software, or applications not related to educational or employment purposes.

5. Offers

a. Family members are not prohibited from clicking any email or pop-up offers without parental consent.

6. Software Use & Copyrighted Material

a. Family members must follow software licensing agreements and abide by copyright restrictions for all software and materials viewed on Hall family electronic assets.

7. Encrypted Files on Electronic Assets

a. No encrypted files are permitted on any electronic assets.

Systems Management

The parents or the person designated by the parents is responsible for the Wireless Local Area Network (WLAN), all electronic device settings, maintenance, firewalls, and malware/virus software.

Violations of Policy

Failure to abide by any of these fair and responsible use policies will result in a warning for first-time violators, followed by disciplinary actions or restrictions on electronic device use for all other occurrences, including a permanent bar. Family members are instructed to report any known violations of these policies to the parents either openly or anonymously.

Policy Review and Modification.

This policy will be reviewed and modified annually based on feedback from family members during the annual family meeting.

Limitations of Liability

The parents or other family members are not responsible for exposure to personal information that was not username and password protected.

Feedback

My uncle is a marketing associate for an ecommerce company in Boston. He said the document was too specific to my family and not general enough for consumption by the public. I made some adjustments by adding more categories under “prohibited use.” I also used an alpha-numerical organization to allow families to add more categories depending on their preferences.

Reference List

Whitman, M. E., & Mattord, H. J. (2018). Management of Information Security (6th ed.). Cengage Learning.

Computer Use and Electronic Information Security Policy < University of Nebraska Medical Center. (n.d.). Retrieved September 21, 2022, from https://catalog.unmc.edu/general-information/student-policies-procedures/it_policy/

Information Security Policy Templates | *SANS Institute*. (n.d.). Retrieved September 25, 2022, from https://www.sans.org/information-security-policy/