WELL FAMILY FITNESS Well Family Fitness

Corporate Proposal V: Security Guidelines

1.0 Overview

Wells Family Fitness strives to uphold values that align with the Christian worldview in every aspect of the company as well as provide employees, customers, and Wells Family Fitness a safe space. In providing these guidelines, employees will be fully informed on the various contributions and responsibilities that play a role in the safety of Wells Family Fitness on a technological level.

2.0 Purpose

This policy aims to outline the security protocols, procedures, and standards at Wells Family Fitness. They are set in place to protect the employee, consumer, and Wells Family Fitness. Inappropriate security procedures may lead Wells Family Fitness to risks including but not limited to compromised network systems, data exposure, services, and legal issues.

3.0 Scope

This policy applies to employees, consultants, temporary staff, remote workers, and other workers at Wells Family Fitness, including all personnel affiliated with the company. This policy applies to all equipment owned or leased by Wells Family Fitness.

4.0 Physical Access

- Physical access to information resources and technology-restricted facilities must be documented and managed
- The person responsible for information resources and technology facilities must review access records and visitor logs for the facility on a periodic basis and investigate unusual accesses.
- Never input unknown devices into Wells Family Fitness laptop, workstation, PC, server or any additional company devices.

5.0 Logon Access

- The administration must create audits to record logon successes and failures, log-offs,
- The administration must create audits to record attempts to use actions that require special administrative permissions.
- Never share your password and username with any employee or co-worker outside of administrators when appropriate.

6.0 Appropriate Usage

- Passwords are set up to expire every 120 days, be sure to recreate a new password each time for the safety of your account, and ultimately Wells Family Fitness.
- Avoid sharing credentials for WiFi, desktop logons, dashboard logons, etc.
- Handle all physical systems with care, damaging any physical components can jeopardize any level of security within a system.

7.0 Malware prevention/detection

- There are many simple ways to prevent malware from entering your desktops and laptops:
    - Do not download free software from the Internet that is not established as secure and relevant by Well Family Fitness
    - Do not open email attachments from outside the company, contractors, unapproved third-party emails, suspiciously labeled, or unexpected.
    - Do not click a fake error message or pop-up window for they can initiate malware downloads

8.0 Auditing

- Auditing is the recording of events that are needed to monitor activity across a network of desktops, laptops, workstations etc.
    - Administrators will preset audits for logon/off activity, account management, policy changes, system events, Active Directory Service Access
    - The previously mentioned audits will help in monitoring and providing records for random password attacks, stolen password attacks, and misuse of privileges.

9.0 Systems updates and Patching

- Patches are software and OS updates that focus on fixing security vulnerabilities within a program. Administrators will routinely install updates as soon as possible to best protect the technological products and software of Wells Family Fitness.
- Administrators must ensure that all technology systems have updated patches installed.
- It is your responsibility to ensure that your programs’ updates are installed and if they are not, contact your administrator.

References

541.pdf on. (n.d.). Egnyte. Retrieved November 7, 2022, from https://sansorg.egnyte.com/dl/FFT45L6ZpR

Computer Security - Policies. (n.d.). Retrieved November 7, 2022, from https://www.tutorialspoint.com/computer_security/computer_security_policies.htm

Hayslip, G. (2018, March 16). *9 policies and procedures you need to know about if you're starting a new security program*. CSO Online. https://www.csoonline.com/article/3263738/9-policies-and-procedures-you-need-to-know-about-if-youre-starting-a-new-security-program.html

Protect yourself from malware - Google Ads Help. (n.d.). Retrieved November 7, 2022, from https://support.google.com/google-ads/answer/2375413?hl=en

SecurityPolicies. (2010, August 17). *How to Write an Information Security Policy in 5 Minutes* [Video]. YouTube. https://www.youtube.com/watch?v=PlRaC78n9f0

Understanding Patches and Software Updates | CISA. (n.d.). Retrieved November 7, 2022, from https://www.cisa.gov/uscert/ncas/tips/ST04-006