Fillosophy Security Plan

Introduction

By definition, network protection is the collection of advancements, cycles, and practices intended to secure organizations, PCs, projects and information from assault, harm or unapproved access. In a processing setting, security incorporates both online protection and actual security. This Security Plan will depict how the security is actualized and characterized, with controls and arrangements. The fundamental reason for this security plan is to give activities that are needed to accomplish the most significant level of security workable for the Fillosophy framework just as to introduce an establishment for its partners.

The goals and ensuing activities of the Fillosophy IT security plan are from a security self-evaluation by the Federal Communications Commissions. The Fillosophy IT Security Plan supplements the Official Security Policies, Standards, and Procedures set up for the Fillosophy System. This security plan is proposed to conform to the guidelines and arrangements set somewhere near the State of California, organization of Fillosophy, the Federal Data Security Management Act (FISMA), and other state and government guidelines.

Authorized Access

Framework access security contains both physical and technical cybersecurity controls which accompany the segment of this arrangement, and will address all parts of accessing in Fillosophy databases.

Technical Systems Access

Identity and Access Management (IAM)

Identity and Access Management, IAM alludes to a structure of approaches and advances for guaranteeing that the correct individuals employed by Fillosophy are granted the accessibility to technology and company resources. For the remainder of this report, the Identity and Access Management will be referred to as IAM.

IAM frameworks ought to encourage the cycle of client provisioning and account arrangement. The item should diminish the time needed with a controlled work process that decreases mistakes and the potential for misuse while empowering robotized account satisfaction. Personality and access to the executive's frameworks ought to likewise furnish the chairmen with the capacity to in a flash view and change access rights.

It may very well be hard to get financing for IAM ventures since they don't straightforwardly build to benefit the company's profitability or usefulness. Lack of identity confirmation and access management pose issues regarding the security of Fillosophy and the compliance of employees; increasing the dange increment the danger of more prominent harms from both external and internal threats.

Email Accounts

Associates received a unique username and email address upon hire. They received this data when they completed hiring papers and introduction orientation with the Fillosophy HR division. At this time, they are aware and acknowledged the policies below:

- Use of Copyrighted Materials
- District Computer and Internet Access
- Social Media and Digital Communications
- Employees are aware of the use of Fillosophy Email Records maintained by the HR division.

The IAM framework set up at Fillosophy sets employee's access levels depending on the division and status they are working as well as their function inside that office. Every employee has their record of being so they should be the only authorized person to have access to their account by any means except if there are unique conditions. To decide whether these conditions are considered suitable, a solicitation must be made to the Technology Services office, and it must be affirmed by both the Technology Services Coordinator and the Executive Leadership Team individual from the mentioning office. An email expressing endorsement will be adequate, and that there should be no sweeping or unrecognizable usernames that permit various unknown logins to the Fillosophy organization.

Password Policy

- Passwords must contain at least 8 characters which must consist of 1 upper case letter as well as 1 numeric value or symbols
- Passwords must be secure, and you will be prompted if the password does not fit requirements or is insecure
- All Fillosophy passwords must only be used on systems regarding the business
- As always, refrain from reusing passwords and disclosing your or others passwords and personal information
- A password will be issued to each employee, but can be changed within the first week of hire

- In the event of loss or compromise security of a password, individuals must contact the IT department for further assistance

Data Communication Security

Data communication is a transmission of data between any technological device linked to the network that can receive data. In regards to Fillosophy, this can be discussing the perimeter security, as well as our protections against viruses, and other malicious software.

Perimeter Security

Perimeter Security and firewalls are safeguards against outside threats from unauthorized access to the network. Network security features such as firewall safeguards networks that access the Internet or third-party services such as Local and Wide Area Network (LAN and WAN). It is a requirement to apply the network security between the LAN and the Virtual Private Network (VPN).

Required security activity to a secure network are:

- Remove default account
- Keep a record of all actions from all devices
- Clearly state a warning into the login banner of the system that unauthorized access is against the law

The Intrusion Detection System (IDS) can enhance security and is a valuable recommendation.

Software Patches

Report, and patch any errors in the platforms of software as soon as possible. If left unpatched, the software must be removed till patched and restored. Renew or replace the software before it reaches its End of Support date or expires: and inform the IT if any changes or updates are made to add in the business's software records.

Protection Against Malicious Software

A measure of security for antivirus, malware, and other unwanted or suspicious software should be introduced on all company products and technology including laptops, desktops, servers, etcetera. This measure must be one that can manage centrally over all of Fillosophy’s gadgets and devices.

Physical Security Measures

Physical security controls and secured regions are utilized to limit unapproved access, harm, and impedance to data and data frameworks. Physical Security implies giving natural shields to controlling any physical admittance to the company's devices and information on the University network to shield data innovation assets from unapproved use, regarding both physical equipment and information points of view.

Physical Entry Security

All areas holding confidential information should not be accessed by an unauthorized person. Entrances must be electronically secured, updated, and re-examined. Unauthorized individuals will be put on leave or further consequences if there's failure to comply with access point rules and security. Ensuring authorized workers' identity beyond the entrance visible identification badges are necessary. Employees who have forgotten their badges or any unauthorized individuals will be escorted out of the data center and handled by administration and security.

Equipment Control

The individual who is responsible for any documents or technology containing sensitive information must notify the department manager if not present in a routine meeting, lent to someone, or anything unfortunate or unprecedented happened to any equipment or data. Sensitive information must always be in a secure area to avoid unfortunate incidents and to ensure that all data and documents of employees and clients are safe and secure. All equipment such as computers and media contain sensitive information and should not be shared as all devices are clearly labeled as property of Fillosophy.

Sensitive Personal Information

The Gramm-Leach-Bliley Act is a precaution measure for Nonpublic Personally Identifiable Financial Information, protecting customers' sensitive data and allows customers to be aware of their data shared and secured information sharing. Fillosophy will execute and clearly state the security of customer's data appropriate to the level of its sensitivity, protecting from harm or intrusion of data privacy.

Warning Signs

Warning signs or Red Flags teaches businesses to be more aware of suspicious activities, which allows further action before identity theft occurs or prevents further damage. Consciously thinking of situations and watching for any warning signs is crucial in order to establish the problem and take steps to prevent any unwanted access from escalating into identity theft, compromising all databases in a data breach.

Payment Security

Payment Card Industry Data Security Standard is a security standard that must be followed to protect the consumer's card payment information during the payment process. Though not required by the law, it's crucial in order to effectively protect all customer's payment information.