Frinksyn-Security Compliances

Table of Contents

1. Introduction:

Our valuable clients are the most important to us. We work really hard to keep your data and private information safe. We want you to trust us and know that we're doing our best to make sure your privacy and security are great. We also want to be clear about how we keep things safe so you can trust us even more. This paper tells you how we keep your private information safe.

2. Principles:

Our product design is driven by the following guiding principles:

1. Minimal Data Gathering:

Our approach involves gathering only essential metadata necessary to furnish administrators with precise insights into SaaS usage within their organization.

2. Clarity:

We ensure absolute transparency by explicitly outlining the data we gather and detailing how it is utilized.

3. Security:

Our unwavering commitment is to safeguard all sensitive data through state-of-the-art technological infrastructure and meticulous processes.

3. Organization & People

Frinksyn maintains an ongoing vigilance over the security well-being of its data. The recruitment of all personnel entails a comprehensive background verification procedure. Additionally, every staff member is obligated to partake in essential security training.

4. Access Control Policy

FRINKSYN LLP sets specific requirements to safeguard information and information systems from unauthorized access. It emphasizes effective communication about the necessity of access control for information and information systems.

- **Purpose:**

Information security shields information from accidental or intentional exposure, alteration, or destruction. Information is a valuable asset for FRINKSYN LLP, demanding careful management. Not all information holds equal value or requires identical protection. Access controls are implemented to safeguard information resources by regulating authorized users and preventing unauthorized use. Formal procedures manage the granting and modification of information access. This policy also enforces a standard for creating strong passwords, their safeguarding, and regular updates.

- **Scope:**

This policy covers all aspects of FRINKSYN LLP, including Organization, Committees, Departments, Partners, Employees (including system support staff with privileged administrative access), contracted third parties, and Organization-affiliated agents. It encompasses any interaction with FRINKSYN LLP information and information systems.

5. E-mail and Internet Security Policy

FRINKSYN LLP establishes specific measures to safeguard internet and email services.

- **Purpose:**

This policy aims to mitigate risks associated with internet and email services. It outlines controls to counter unauthorized access, information theft, service theft, and malicious service disruption.

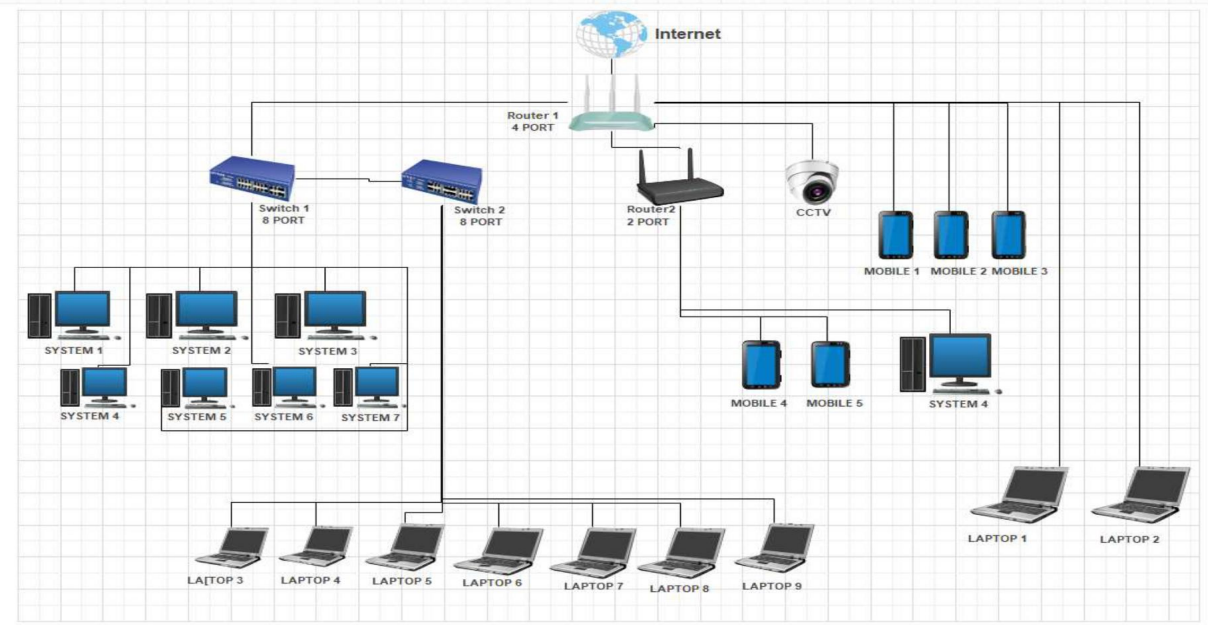
- **Scope:**

Applicable to all users of information assets, including FRINKSYN LLP employees, temporary agency workers, vendors, business partners, contractor personnel, and functional units worldwide.

The policy encompasses all Information Systems environments managed by FRINKSYN LLP or third parties under contract. "IS environment" refers to the complete setting, including documentation, physical/logical controls, personnel, software, and information.

While this policy details user responsibilities, it's not exhaustive. Other FRINKSYN LLP Information Security policies, standards, and procedures assign additional duties. Users must comprehend and adhere to these documents. Queries should be directed to relevant personnel like systems administrators, managers, or HR, who can contact the Information Security Department for clarification. Conflicts arising from this policy will be resolved by the Information Security Department.

6. Network Architecture



Frinksyn operates primarily through the Internet, utilizing the subsequent network elements:

1. The primary internet connection is established via "Router 1," equipped with 4 ports. This hub links to:
- Three mobile devices ("Mobile1," "Mobile2," "Mobile3").
- One Closed-Circuit Television (CCTV) system.
- Another networking node, "Router 2," featuring 2 ports.
- Two laptops ("Laptop 1," "Laptop 2").

2. The network distribution is facilitated by "Switch 1," which has 8 ports and is connected to "Router 1." It interconnects:
- Seven systems ("System 1" to "System 7").

3. "Router 2" plays a role in extending connectivity to:
- Two mobile devices ("Mobile4," "Mobile5").
- One additional system ("System 4").

4. Expanding the network further is an additional 8-port entity, "Switch 2," linked to "Switch 1." It accommodates connectivity for:
- Seven laptops ("Laptop 3" to "Laptop 9").

This intricate network setup fosters efficient communication and collaboration among the diverse array of devices and systems that constitute the Frinksyn network.

7. Password Security policy

Passwords play a pivotal role in computer security, acting as the primary defense for user accounts. A poorly chosen password could jeopardize the entire network of FRINKSYN LLP. Hence, all FRINKSYN LLP personnel (including contractors and vendors with system access) must follow the outlined steps to wisely select and protect their passwords.

- **Purpose:**

This policy establishes a standard for generating robust passwords, ensuring their safeguarding, and determining their change frequency.

- **Scope:**

This policy extends to all end-users and personnel who possess or are accountable for an account (or any access needing a password) on any system/service within the NIC domain. This encompasses personnel with designated desktop systems and also covers application designers and developers.

8. Compliances

Frinksyn possesses the essential support from individuals, procedures, and technology required to safeguard customer personal data, ensuring adherence to legal and contractual responsibilities encompassing regulations like ISO.

ISO 27001-2013:

Frinksyn holds ISO 27001 certification granted by an independent third party. This certification serves as a foundation for identifying, overseeing, fortifying, and enhancing SaaS applications. The International Standard outlines the prerequisites for creating, executing, upholding, and iteratively enhancing an information security management system within the organization's scope. Furthermore, this standard incorporates criteria for evaluating and addressing information security risks, tailored to suit the specific requirements of Frinksyn.

You can review our ISO Certificate here.

9. Conclusion

In conclusion, this paper highlights the company's strong commitment to safeguarding client data privacy and security. The document emphasizes transparency in data practices and praises the company's responsible approach to data collection. Security measures are underscored, reassuring clients about data protection. This approach aligns with industry standards and legal requirements, establishing the company as a trustworthy guardian of client data. In a digital era focused on privacy, the company's efforts set a positive example for peers, demonstrating dedication to exceeding client expectations for data security