



Information Security Regulations of Future Concept SAC

Introduction

This regulation aims to establish the necessary measures and actions to guarantee the protection of Future Concept SAC's information and related assets against unauthorized access, misuse, disclosure, and alteration. This regulation is based on Future Concept SAC's information security policy and applies to all business areas, employees, contractors, suppliers, and third parties who interact with the organization.

Identification of Information Assets

Future Concept SAC will identify and document all relevant information assets and their owners. The classification of information will be based on its importance, sensitivity, and level of risk. Information assets will be labeled with an appropriate classification and adequate access controls will be established.

Access to Information

Access to information will be limited to those who need to access it to perform their functions and responsibilities. Access rights will be granted based on the necessity of knowing the information to perform job-related tasks. Access will be revoked when no longer necessary or when a security breach occurs.

Password Policy

Future Concept SAC will establish a password policy that includes password complexity, change periodicity, prohibition of password reuse, the need for secure passwords on critical systems, and the limitation of login attempts.

Protection of Information Assets

Future Concept SAC will establish adequate security controls to protect information assets against loss, destruction, corruption, theft, or damage. These controls will include appropriate physical, technical, and organizational security measures for the classification and level of risk of information assets.

Network Security Policy

Future Concept SAC will establish a network security policy that includes protection of the network against malicious attacks and management of network device security. Network devices will be configured according to security best practices and updated regularly to protect against known vulnerabilities.

Information Security Incident Management

Future Concept SAC will establish and maintain a process for reporting, investigating, and responding to information security incidents. All information security incidents will be reported to Future Concept SAC's information security management system (ISMS) responsible person. Measures will be taken to prevent the recurrence of information security incidents.

Mobile Device Use

Any employee who uses a mobile device (such as a smartphone, tablet, or laptop) to access Future Concept SAC's information must protect the device with a secure password and data encryption. Mobile devices must be kept up-to-date with the latest security patches and updates. Employees must immediately report if they lose a mobile device containing Future Concept SAC's information or if it is stolen.

Backup and Restoration

Future Concept SAC will regularly perform backups of information and systems to ensure recovery in case of disruptions or disasters. Employees must follow backup and restoration policies and procedures to ensure the integrity and availability of information.

Analysis and Monitoring

Future Concept SAC will regularly perform analysis and monitoring of information and systems to detect and prevent potential security threats. Employees must immediately report any suspicious or unusual activity they may detect.

Security Testing

Future Concept SAC will regularly perform security testing on systems and applications to detect potential vulnerabilities and ensure the effectiveness of security controls. Employees must follow security testing policies and procedures to ensure information security.

Reviews and Audits

Future Concept SAC will conduct regular reviews and audits of the information security management system to ensure its effectiveness and compliance with policies and procedures. Employees must cooperate with reviews and audits by providing necessary information and data.

Legal and Contractual Compliance

Future Concept SAC will comply with applicable laws, regulations, and standards related to information security and ensure compliance with contractual requirements related to information security. Employees must follow policies and procedures to ensure legal and contractual compliance.

Consequences of Non-Compliance

Future Concept SAC reserves the right to take disciplinary action, including termination of employment, against any employee who violates the information security policy. Employees are responsible for reporting any violation of the information security policy to their immediate supervisor or the person in charge of the information security management system.

Review and update

Future Concept SAC will regularly review and update the information security policy and regulations to ensure their effectiveness and relevance. Employees must be aware of changes to the policy and regulations and follow updated procedures.

Lima, October 01/2022.



+51 992 743 849



Av. Santo Toribio 143, 2do piso – Oficina 55
San Isidro, Lima – Perú



innovacion@futurelab.pe

www.futurelab.la

