



SI Instruction Manual for Future Concept SAC

INSTRUCTION 1: Instructions for identifying and evaluating information security risks and applying measures to mitigate them

I. Objective:

The objective of this instruction is to provide a framework for identifying and evaluating information security risks, as well as for applying measures that allow them to be mitigated, in order to ensure the confidentiality, integrity, and availability of Future Concept SAC's information assets.

II. Scope:

This instruction applies to all business areas, employees, contractors, suppliers, and third parties who handle information assets with Future Concept SAC, including printed and electronic information, data storage and processing devices.

III. Procedure

1. **Identification of information assets:** A comprehensive list of all information assets handled in the organization must be prepared, including printed and electronic information, as well as data storage and processing devices.
2. **Identification of threats and vulnerabilities:** All possible threats and vulnerabilities that may affect the organization's information security must be identified. Some sources of threats and vulnerabilities include the nature of the business, the physical location of the organization, the technology used, and personnel.
3. **Risk assessment:** Once information assets, threats, and vulnerabilities have been identified, the risk associated with each information asset must be evaluated. This is done by determining the probability and impact of each threat or vulnerability on the information assets.
4. **Selection of security measures:** After evaluating the risks, appropriate security measures should be selected to mitigate the identified risks. These measures may include technical, administrative, and physical controls.
5. **Implementation of security measures:** Once appropriate security measures have been selected, they must be implemented to ensure that information security is maintained at all times.

6. **Monitoring and review:** A continuous monitoring and review process should be established to ensure that implemented security measures are effective and adapt to changes in the organization and its environment.
7. **Update of risk assessment:** A periodic review of the risk assessment should be conducted to ensure that risks are mitigated and that security measures remain effective.

IV. Conclusion:

It is important that all organization personnel are aware of the importance of maintaining information security and are trained in the procedures established in this instruction. Additionally, a process for reporting and responding to information security incidents should be established to act quickly in any eventuality.

INSTRUCTIONS 2: Instructions for the identification of information assets in Future Concept SAC

I. Objective:

This instruction aims to guide employees, contractors, suppliers and third parties who interact with Future Concept SAC in the process of identifying the information assets of the organization.

II. Scope:

This instruction applies to all business areas, employees, contractors, suppliers and third parties that interact with Future Concept SAC.

III. Responsibility:

The personnel designated by Future Concept SAC will lead the process of identifying the organization's information assets. Employees, contractors, suppliers, and third parties who interact with Future Concept SAC have the responsibility to actively participate in this process.

IV. Procedure:

1. **Identification of information assets:** Information assets are valuable elements for the organization and must be protected. To identify them, a list should be made that includes:
 - a. Confidential information, such as personal data, financial information, business strategies, among others.
 - b. Information systems, such as applications, databases, servers, among others.
 - c. Network infrastructure, such as routers, switches, firewalls, among others.
 - d. Mobile devices, such as smartphones, tablets, laptops, among others.
 - e. Storage media, such as external hard drives, USB flash drives, CD, DVD, among others.
 - f. Physical documents, such as contracts, invoices, records, among others.
2. **Categorization of information assets:** Once the information assets have been identified, they should be categorized according to their importance and level of risk to the organization. Categorization will allow the establishment of adequate security measures to protect them.

Criteria such as financial impact, strategic relevance, market value, confidentiality, among others, can be used.

3. **Updating the list of information assets:** The list of information assets should be updated regularly to include new information assets and eliminate those that are no longer necessary. Updating the list is important to ensure that the organization has a clear and up-to-date view of the information assets it possesses and must protect.
4. **Communication and awareness:** It is important that all employees, contractors, suppliers, and third parties who interact with Future Concept SAC are informed about the list of information assets and their importance to the organization. Therefore, a communication and awareness campaign should be carried out to sensitize all stakeholders about the importance of protecting information assets and the risks associated with their loss, theft, or unauthorized disclosure.

V. Conclusions:

The identification of information assets is a fundamental process to establish adequate security measures and protect the organization's information. It is important that all employees, contractors, suppliers, and third parties who interact with Future Concept SAC actively participate in this process and are informed about its importance.

INSTRUCTION 3: Instructions for Secure, Confidential, and Integral Access and Handling of Information at Future Concept SAC

I. Objective:

This instruction aims to establish procedures for secure, confidential, and integral access and handling of information at Future Concept SAC.

II. Scope:

This instruction applies to all employees, contractors, consultants, and other third parties who access, handle, or process information on behalf of Future Concept SAC.

III. Procedure:

1. **Access to Information:** Access to information should only be granted to employees who need the information to perform their job duties. Each employee must have unique and confidential access credentials assigned according to the level of access required.
2. **Access Control:** Future Concept SAC must establish physical and logical access controls to ensure that only authorized personnel are allowed access to the information. Access credentials should be assigned in accordance with company policies and procedures.
3. **Information Protection:** Security measures must be established to protect the information from unauthorized disclosure, destruction, or alteration. This may include the use of secure passwords, encryption of information, and implementation of physical and logical access controls.
4. **Proper Use of Information:** Access to information should only be used for legitimate and authorized purposes. Employees must respect the confidentiality of the information and not disclose it to unauthorized third parties. Additionally, information should not be copied, deleted, or altered without appropriate authorization.
5. **Access Removal:** Access to information should be removed when the employee no longer needs it to perform their job duties or if the employee ceases to work for Future Concept SAC. Access removal should be performed in a timely and complete manner to ensure that the information is not exposed to unnecessary risks.
6. **Training and Awareness:** All employees must be trained and made aware of policies and procedures for access and handling of information.



Training should be offered regularly to ensure that all employees are aware of best practices for information security.

IV. **Compliance:**

All employees, contractors, consultants, and other third parties who access, handle, or process information on behalf of Future Concept SAC must comply with the policies and procedures established for access and handling of information. Non-compliance with these policies and procedures may result in disciplinary and legal actions.

INSTRUCTION 4: Password Policy Guidelines at Future Concept SAC

I. Objective:

The aim of this instruction is to establish policies and procedures to ensure that all passwords used within the organization are secure and adequately protected.

II. Scope:

These policies apply to all employees, contractors, and third parties who use passwords to access systems and data at Future Concept SAC.

III. Procedure:

1. **Password Complexity Requirements:** All passwords must meet the following requirements:
 - a. Have a minimum length of eight characters.
 - b. Include at least one uppercase and one lowercase letter.
 - c. Include at least one number or symbol.
2. **Password Changes:** Passwords must be changed every 90 days. Users must be notified in advance so they can change their passwords before they expire.
3. **Prohibition on Sharing Passwords:** Passwords must never be shared with third parties, including other employees or contractors of Future Concept SAC.
4. **Safe Password Storage:** Passwords must never be stored in plain text. They must be stored securely, using appropriate encryption techniques.
5. **Use of Strong Passwords for Administrator Accounts:** Administrator accounts must use especially strong passwords to protect critical systems of Future Concept SAC.
6. **Restriction of Login Attempts:** The system must be configured to automatically block an account after a specific number of failed login attempts.
7. **Password Integrity Verification:** Systems must verify password integrity to prevent the use of compromised passwords.

8. **Security Violation Notification:** Employees must be trained to report any suspicion of security violation or password compromise to the information security management.

IV. Conclusion

These policies and procedures will help ensure that passwords used by Future Concept SAC are secure and adequately protected. All employees, contractors, and third parties who use passwords in the organization must follow these policies and procedures at all times.

INSTRUCTION 5: Instruction for the Information Asset Protection Policy in Future Concept SAC.

I. Objective:

This instruction aims to establish the necessary protection measures to ensure the security of information assets in Future Concept SAC.

II. Scope:

This instruction applies to all employees and contractors of Future Concept SAC who have access to the organization's information assets.

III. Procedures:

1. **Classification of information assets:** All information assets must be classified according to their importance and sensitivity level. The classification should be based on factors such as confidentiality, integrity, and availability of the information.
2. **Access and control of information assets:** Access controls for information assets must be established according to their classification. Controls may include authentication, authorization, and supervision of users accessing information assets.
3. **Proper use of information assets:** A clear policy on the proper use of information assets must be established. Employees and contractors must be aware of the policies and procedures they must follow to use the organization's information assets.
4. **Physical protection of information assets:** Physical protection measures for information assets must be established. These measures may include restricting physical access to information assets and protection against theft, fire, or environmental damage.
5. **Logical protection of information assets:** Logical protection measures for information assets must be established. These measures may include protection against computer viruses, cyber-attacks, and other security risks.
6. **Use of secure storage and transportation media:** Measures must be established for the safe use of information storage and transportation media such as external hard drives, USBs, or emails. Employees and contractors must use only authorized and adequately protected media.

7. **Secure information elimination procedures:** Procedures must be established for the secure elimination of information assets when no longer needed. These procedures must ensure that information is securely deleted and cannot be recovered.

IV. Conclusion:

The implementation of appropriate policies and protective measures for information assets is essential to ensure the security of information at Future Concept SAC. It is important that all employees, contractors, and third parties are committed to information security and comply with the established policies and measures.

INSTRUCTION 6: Instructions for network security policy in Future Concept SAC

I. Objective:

Ensure the security of the Future Concept SAC network and the information transmitted through it.

II. Scope:

This policy applies to all network devices, including mobile devices, that are used to access the network of Future Concept SAC.

III. Procedures:

- 1. Network Protection:** Technical, administrative, and physical security measures must be implemented to protect the network of Future Concept SAC. These measures may include, but are not limited to:

- a. Firewalls.
- b. Packet filtering.
- c. Antivirus and antimalware software.
- d. Regular patch updates and security updates.
- e. Network segregation and segmentation.
- f. Network access control.
- g. Monitoring and recording of network activities.
- h. Verification of the security of mobile devices accessing the network of Future Concept SAC.

- 2. Network access:** Access to the network of Future Concept SAC should only be allowed to authorized employees who need it to perform their work functions. Employees must authenticate before gaining access to the network and appropriate access levels should be established for each employee.

- 3. Monitoring and recording of activities:** All activity on the network of Future Concept SAC must be monitored and recorded to detect possible threats and security violations. Clear policies on acceptable network use must be established and employees should be trained on these policies.

- 4. Incident response:** A response plan must be established to address any possible network security violation. This plan should include the identification of possible threats, the assignment of response responsibilities, and the definition of communication and notification processes.

5. **Business continuity:** Business continuity measures must be implemented to ensure that the network of Future Concept SAC continues to operate in case of a security incident. These measures may include, among others, regular backups of critical information and the implementation of a disaster recovery plan.

IV. Conclusion:

The network security policy of Future Concept SAC is essential to ensure the security of information transmitted through the network. Protecting the network and implementing appropriate security measures are essential to ensure uninterrupted network operations. User authentication and implementation of appropriate access levels are important to protect organizational information and minimize security risks. Monitoring and logging of activities and implementation of business continuity measures are essential to ensure that the network of Future Concept SAC continues to operate in the event of a security incident.

INSTRUCTION 7: Instructions for the Management of Information Security Incidents at Future Concept SAC.

I. Objective:

The objective of these instructions is to establish a process for the management of information security incidents at Future Concept SAC in order to minimize damage and restore affected services in case of an information security incident.

II. Scope:

These instructions are applicable to all employees and contractors of Future Concept SAC who work with organization information.

III. Procedures:

1. **Incident notification:** Any employee or contractor who observes an information security incident must immediately notify the information security instance of Future Concept SAC, which is responsible for the operations area.
2. **Initial evaluation:** The information security instance of Future Concept SAC must conduct an initial evaluation of the incident to determine its nature, scope, and possible impacts.
3. **Containment:** Immediate measures must be taken to contain the incident and minimize its impact. This may include the suspension of services or the isolation of affected systems.
4. **Investigation:** A thorough investigation of the incident must be conducted to determine its root cause and how it could be prevented in the future.
5. **Notification and communication:** The affected stakeholders must be notified of the incident and the investigation results communicated. This may include clients, suppliers, and other related parties.
6. **Restoration:** Measures must be taken to restore affected services and minimize the impact on the organization. This may include data recovery, system restoration, and equipment repair.
7. **Lessons learned analysis:** After the incident, a lessons learned analysis must be conducted to identify areas for improvement and opportunities to strengthen information security measures at Future Concept SAC.

8. **Policy and procedures update:** Future Concept SAC's information security policies and procedures must be updated as necessary to address the areas for improvement identified in the lessons learned analysis.

IV. Update:

These instructions for the management of information security incidents at Future Concept SAC must be regularly reviewed and updated to ensure their effectiveness and relevance.

INSTRUCTION 8: Instructions for Backup and Restore Management at Future Concept SAC

I. Objective:

The purpose of this instruction is to establish the necessary procedures and measures to ensure the proper execution of backup copies of information and its corresponding restoration in the event of a service interruption.

II. Scope:

This instruction is applicable to all employees and contractors of Future Concept SAC who manage and/or administer information on computer systems and devices, as well as to the IT teams responsible for backup and restore management.

III. Procedures:

1. **Backup Planning:** Adequate planning must be carried out for the execution of backup copies, which must include the frequency of backup execution, the type of backup to be carried out, and the storage medium to be used. In addition, recovery procedures and tests must be defined to verify the effectiveness of backup copies.
2. **Selection of Storage Medium:** A reliable and secure storage medium must be selected to store backup copies, such as external hard drives, network storage devices (NAS), or cloud storage services.
3. **Backup Execution:** Backup copies must be regularly executed in accordance with the previously established plan. To do this, backup software or specific tools must be used to carry out backup copies on command lines.
4. **Verification of Backup Copies:** Regular tests must be carried out to verify the integrity and quality of the backup copies made. In addition, backup copies must be regularly verified to ensure that they have been correctly made and can be restored without any issues.
5. **Protection of Backup Copies:** Adequate measures must be taken to protect backup copies, such as using secure passwords and implementing physical security measures to prevent their loss, theft, or damage.
6. **Restore Procedures:** Clear procedures must be established for restoring backup copies in the event of a service interruption or data loss. These

procedures must be known by all personnel involved in backup and restore management.

7. **Restore Testing:** Regular tests must be carried out to verify the effectiveness of backup copies and restore procedures. These tests must be carried out by trained personnel and properly documented.
8. **Backup Update:** Backup copies must be regularly updated to ensure that the most recent data is included. Clear procedures must be established for backup updating and followed rigorously to ensure the integrity of information.

IV. Conclusion

Proper management of backup copies and their corresponding restoration are fundamental to ensure business continuity in the event of a service interruption or data loss. Therefore, it is important to follow established procedures and conduct regular tests to ensure the effectiveness of backup copies and restore procedures.

INSTRUCTION 9: Instructions for Information Security Analysis and Monitoring at Future Concept SAC

I. Objective:

The objective of this instruction is to establish procedures for the analysis and monitoring of information security at Future Concept SAC, in order to detect and prevent possible security incidents and continually improve security controls.

II. Scope:

This instruction applies to all areas and users of Future Concept SAC that handle organizational information.

III. Procedures:

1. **Identification of critical points:** Identify critical points in the organization's infrastructure, such as servers, databases, and applications, which require constant monitoring to detect possible threats and vulnerabilities.
2. **Selection of monitoring tools:** Select appropriate monitoring tools for each critical point that allow for the collection and analysis of relevant information for information security.
3. **Establishment of alert thresholds:** Establish alert thresholds for each monitoring tool so that an alert is triggered when unusual or suspicious activity is detected at critical points.
4. **Analysis of alerts:** When an alert is received, the collected information must be analyzed to determine whether it is a real threat or a false alarm.
5. **Actions in response to incidents:** In case of confirming a security incident, necessary measures must be taken to mitigate the effects of the incident and prevent its spread. A specific procedure must be established for each type of incident, which includes notifying the involved parties and recovering affected data.
6. **Continuous monitoring:** Information security must be constantly monitored by periodically reviewing security controls and updating monitoring and analysis procedures based on new threats and vulnerabilities.
7. **Incident logging:** Maintain a detailed record of all security incidents detected and actions taken to resolve them, in order to track and evaluate the effectiveness of implemented measures.

IV. Conclusion

Information security analysis and monitoring is a crucial process for detecting and preventing possible security incidents at Future Concept SAC. Implementation of appropriate monitoring tools and clear procedures for incident analysis and management will improve information security and ensure business continuity. It is important to remember the importance of staying updated on new threats and vulnerabilities and continuously adapting security controls to protect organizational information.

INSTRUCTION 10: Instruction for conducting security tests at Future Concept SAC**I. Objective:**

The purpose of this Instruction is to establish the necessary Procedures for conducting security tests at Future Concept SAC, in order to identify potential vulnerabilities and risks in the organization's systems and applications.

II. Scope:

This Instruction applies to all systems and applications used at Future Concept SAC and to any person conducting security tests in the organization.

III. Procedures:**1. Security test planning:**

- a. Identify the systems and applications that will be assessed.
- b. Define the scope of the test and the specific objectives to be achieved.
- c. Establish a schedule for the security test.
- d. Identify the personnel responsible for conducting the tests and define their roles and responsibilities.

2. Information gathering:

- a. Obtain information about the systems and applications to be assessed, such as architecture, configuration, software, and hardware used.
- b. Conduct an assessment of the systems and applications to identify potential vulnerabilities.

3. Vulnerability analysis:

- a. Use vulnerability analysis tools to identify potential vulnerabilities in the systems and applications.
- b. Conduct penetration testing to verify the exploitability of identified vulnerabilities.

4. Risk evaluation:

- a. Use vulnerability analysis tools to identify potential vulnerabilities in the systems and applications.
- b. Conduct penetration testing to verify the exploitability of identified vulnerabilities.

5. Results reporting:

- a. Document the results of the security tests, including identified vulnerabilities and recommendations for mitigating risks.
- b. Present the results to the organization's management and those responsible for the evaluated systems and applications.
- c. Establish an action plan to address identified vulnerabilities and mitigate associated risks.

1. Monitoring and follow-up:

- d. Conduct ongoing monitoring of the systems and applications to detect potential vulnerabilities and risks.
- e. Conduct periodic security tests to verify the effectiveness and adequacy of implemented mitigation measures.

IV. Conclusion:

Conducting security tests is essential to ensure the protection of the systems and applications used in the organization. By following this Instruction, Future Concept SAC can identify potential vulnerabilities and risks in its systems and applications, as well as establish mitigation measures to ensure information security at all times.

INSTRUCTION 11: Instructions for legal and contractual compliance in Future Concept SAC

I. Objective:

The objective of these instructions is to ensure that Future Concept SAC complies with all laws, regulations, and contractual agreements that apply to the company and the information it handles.

II. Scope:

These instructions apply to all areas of the company that handle information, including personnel, systems, and processes.

III. Procedures:

1. **Identification of legal and contractual requirements:** A complete list of all laws, regulations, and contractual agreements that apply to the company and the information it handles must be created.
2. **Compliance evaluation:** Once the requirements have been identified, an evaluation must be performed to determine compliance. This evaluation should be conducted periodically.
3. **Implementation of measures to comply with requirements:** If areas of non-compliance are identified, measures must be implemented to ensure compliance. These measures may include changes in processes, systems, and policies, as well as personnel training.
4. **Review of contracts and agreements:** A periodic review of contracts and agreements with third parties must be conducted to ensure contractual requirements are being met in terms of information security.
5. **Updating of policies and procedures:** If changes in laws and regulations that affect the company and the information it handles are identified, policies and procedures must be updated to ensure compliance.
6. **Establishment of controls:** The following controls must be established:
 - a. **Documentation of policies and procedures:** An updated documentation of all policies and procedures that apply to legal and contractual compliance must be maintained.
 - b. **Personnel training:** Personnel must be trained to understand the legal and contractual requirements that apply to the company and the information it handles.

- c. **Supervision and monitoring:** Mechanisms for supervision and monitoring must be established to ensure legal and contractual requirements are met.

IV. Conclusion:

Legal and contractual compliance is essential to ensure information security and business continuity. Future Concept SAC must implement measures to ensure compliance with all laws, regulations and contractual agreements that apply to the company and the information it handles.

CONTRACTUAL GUIDELINES 1: Contractual Clauses for Third Party Collaborators and Contractors around Software as a Service (SaaS) developed by Future Concept SAC

In the event that the contractor, third party, or collaborator uses any Software as a Service provided by Future Concept SAC, they agree to comply with the following clauses:

- I. **CLAUSE 1: USE OF THE SOFTWARE.** The contractor, third party, or collaborator agrees to use the software provided by Future Concept SAC in accordance with the following guidelines:
 1. Use the software only for the purposes established in the contract and in compliance with Future Concept SAC's information security policy and regulations.
 2. Do not transfer, assign, or sublicense the use of the software to third parties without the prior written authorization of Future Concept SAC.
 3. Immediately report to Future Concept SAC any security incidents related to the Software as a Service, providing all necessary information for analysis and resolution.
 4. Comply with the privacy and data protection policies of the Software as a Service provided by Future Concept SAC.
 5. Use secure and robust passwords to access the software, avoiding sharing them with third parties and immediately notifying any suspicion of compromise of their credentials.
- II. **CLAUSE 2: DURATION OF THE CONTRACT.** The contractor, third party, or collaborator agrees to comply with the clauses established in this document during the entire term of the contract, including extension or renewal periods.
- III. **CLAUSE 3: BREACH OF THE CLAUSES.** In the event that the contractor, third party, or collaborator fails to comply with any of the clauses established in this document, Future Concept SAC reserves the right to take necessary measures to protect its information assets and ensure compliance with the information security policy and regulations, including early termination of the contract.
- IV. **CLAUSE 4: JURISDICTION AND APPLICABLE LAW.** This contract will be governed and interpreted in accordance with the laws of the jurisdiction corresponding to the location of Future Concept SAC, and the parties submit to the exclusive jurisdiction of the courts of that jurisdiction.

This document is integrated into the contract between Future Concept SAC and the contractor, third party or collaborator, and must be signed by both parties as an annex to the main contract.

CONTRACTUAL GUIDELINES 2: Clauses to include in the Partner's contract

- I. **CLAUSE 1: COMPLIANCE.** The collaborator agrees to comply with Future Concept SAC's information security policy and regulations at all times during the term of the contract. Additionally, they agree to follow all established processes and procedures by Future Concept SAC to ensure information security and data privacy.
- II. **CLAUSE 2: USE OF THE INFORMATION.** The collaborator agrees to use the information provided by Future Concept SAC solely for the purposes established in the contract. Furthermore, they commit to maintaining the confidentiality and privacy of the information and not to disclose, transfer, or use it for purposes other than those agreed upon.
- III. **CLAUSE 3: PROTECTION OF ASSETS.** The collaborator agrees to protect Future Concept SAC's information assets, both physical and electronic, under their custody, by preventing their loss, theft, modification, unauthorized disclosure, or destruction. They also commit to reporting any information security incident that occurs in the course of their activities.
- IV. **CLAUSE 4: USE OF PASSWORDS.** The collaborator agrees to use secure and robust passwords for access to Future Concept SAC's systems and applications, avoiding sharing their access credentials with third parties. They also commit to regularly changing their passwords and immediately notifying any suspicion of compromise of their credentials.
- V. **CLAUSE 5: USE OF NETWORKS AND SYSTEMS.** The collaborator agrees to use Future Concept SAC's networks and systems only for the purposes established in the contract, avoiding unauthorized access, introducing viruses, malware, or any other malicious code into Future Concept SAC's systems. They also commit to reporting any network security incidents they detect.
- VI. **CLAUSE 6: NOTIFICATION OF SECURITY INCIDENTS.** The collaborator agrees to immediately notify Future Concept SAC of any information security incident detected during the course of their activities, providing all necessary information for analysis and resolution.
- VII. **CLAUSE 7. MONITORING.** The collaborator agrees to fully cooperate with Future Concept SAC in any investigation or audit related to information security, providing all required information and collaborating in the implementation of any corrective action that may be required.
- VIII. **CLAUSE 8: BREACH OF CLAUSES.** The collaborator acknowledges and agrees that the breach of any information security clause established in this contract may be grounds for termination of the contract and may have adverse legal and financial consequences for both the collaborator and Future Concept SAC.

- IX. **CLAUSE 9: RETURN OF INFORMATION ASSETS.** The collaborator acknowledges and agrees that, in the event of contract termination, they must return to Future Concept SAC all information, materials, and information assets under their custody, as well as any copy or record thereof.
- X. **CLAUSE 10. RIGHT TO MODIFY AND UPDATE.** The collaborator acknowledges and agrees that Future Concept SAC reserves the right to modify and update the information security clauses established in this contract at any time, and that it is responsibility of the collaborator to be aware of any changes and comply with the new provisions established.

CONTRACTUAL GUIDELINES 3: Future Concept SAC clause s for contracts with third parties

- I. **CLAUSE 1: CONFIDENTIALITY.** The third party agrees to maintain the confidentiality and privacy of all information to which they have access under the contract, whether in verbal, written, electronic, or any other format.
- II. **CLAUSE 2: INFORMATION PROTECTION.** The third party agrees to protect Future Concept SAC's information assets, both physical and electronic, that are under their custody, avoiding their loss, theft, modification, unauthorized disclosure, or destruction.
- III. **CLAUSE 3: USE OF INFORMATION.** The third party agrees to use the information provided by Future Concept SAC solely for the purposes established in the contract and not for any other purpose, without the express and written authorization of Future Concept SAC.
- IV. **CLAUSE 4: ACCESS TO INFORMATION.** The third party agrees to use Future Concept SAC's information and systems only for the purposes established in the contract and not to access any other information or system without the express and written authorization of Future Concept SAC.
- V. **CLAUSE 5: PASSWORD POLICY.** The third party agrees to use strong and robust passwords to access Future Concept SAC's systems and applications, avoiding sharing their access credentials with third parties. Likewise, they agree to regularly change their passwords and to immediately notify any suspicion of compromise of their credentials.
- VI. **CLAUSE 6: INCIDENT MANAGEMENT.** The third party agrees to immediately notify Future Concept SAC of any information security incident detected during the development of their activities, providing all necessary information for its analysis and solution.
- VII. **CLAUSE 7: REGULATORY COMPLIANCE.** The third party agrees to comply with all applicable laws and regulations related to information security, including, without limitation, personal data protection regulations.
- VIII. **CLAUSE 8: AUDIT.** Future Concept SAC reserves the right to audit the third party's information security at any time during the contract's validity period, to ensure that the third party is complying with the obligations established in the contract.
- IX. **CLAUSE 9: DURATION OF COMMITMENT.** The obligations established in the contract will remain in force while the third party has access to Future Concept SAC's information or systems, even after the contract's termination.

CONTRACTUAL GUIDELINES 4: Information Security Clauses for Future Concept SAC Contractors

This document aims to establish the clauses that must be included in contracts with contractors working with Future Concept SAC, in order to ensure compliance with the information security policy and regulations, as well as the specifications related to the use of company-owned software and hardware.

- I. **CLAUSE 1: INFORMATION SECURITY POLICY AND REGULATIONS.** The contractor undertakes to comply with Future Concept SAC's information security policy and regulations at all times during the term of the contract.
- II. **CLAUSE 2: ACCESS TO INFORMATION.** The contractor must commit to using the information provided by Future Concept SAC solely and exclusively for the purposes established in the contract. Similarly, they commit to maintaining the confidentiality and privacy of the information, as well as not disclosing, transferring, or using it for purposes other than those agreed upon.
- III. **CLAUSE 3: PROTECTION OF INFORMATION ASSETS.** The contractor undertakes to protect Future Concept SAC's information assets, both physical and electronic, that are under their custody, avoiding their loss, theft, modification, unauthorized disclosure, or destruction. They also commit to reporting any information security incidents that occur during the course of their activities.
- IV. **CLAUSE 4: PASSWORD POLICY.** The contractor undertakes to use secure and robust passwords to access Future Concept SAC's systems and applications, avoiding sharing their access credentials with third parties. They also commit to regularly changing their passwords and immediately notifying any suspicion of compromise of their credentials.
- V. **CLAUSE 5: NETWORK SECURITY.** The contractor undertakes to use Future Concept SAC's networks and systems only for the purposes established in the contract, avoiding unauthorized access, the introduction of viruses, malware, or any other malicious code into Future Concept SAC's systems. They also commit to reporting any network security incidents they detect.
- VI. **CLAUSE 6: INFORMATION SECURITY INCIDENT MANAGEMENT.** The contractor undertakes to immediately notify Future Concept SAC of any information security incidents detected during the course of their activities, providing all necessary information for their analysis and resolution.
- VII. **CLAUSE 7: INFORMATION SECURITY AUDITS.** Future Concept SAC reserves the right to conduct information security audits of the contractor during the term of the contract, in order to verify compliance with the information security clauses established in this document. The contractor undertakes to actively collaborate in the audits and provide all necessary information.

- VIII. **CLAUSE 8: CONFIDENTIALITY.** The contractor undertakes to maintain the confidentiality of all confidential information of Future Concept SAC to which they have access during the course of the contract and not to disclose, transfer, or use it for purposes other than those agreed upon.
- IX. **CLAUSE 9: OWNERSHIP.** The contractor acknowledges that all software and hardware owned by Future Concept SAC and used in the course of the contract remains the exclusive property of Future Concept SAC, and they do not acquire any ownership rights over it.
- X. **CLAUSE 10: TERMINATION OF CONTRACT.** This contract may be terminated by either party upon written notice to the other party with a minimum of thirty (30) calendar days' advance notice. Upon termination of the contract, these guidelines must be followed:
1. If this contract is terminated by either party, the contractor shall deliver to Future Concept SAC all information, documentation, and materials provided by Future Concept SAC, as well as any other assets owned by Future Concept SAC in its possession, within a maximum period of five (5) business days from the date of termination of the contract.
 2. The contractor acknowledges that termination of the contract does not release them from obligations of confidentiality, information security, and protection of Future Concept SAC's assets that they have acquired during the contract's validity, and that they will remain responsible for any breach of such obligations.
 3. Termination of the contract does not exempt the contractor from any liability they have incurred with Future Concept SAC prior to the termination date and shall be responsible for any damage, loss, or harm caused by the breach of their contractual obligations up until the termination of the contract.
- XI. **CLAUSE 11: APPLICABLE LAW.** This contract shall be governed and interpreted in accordance with the laws of the Republic of Peru, without regard to its principles of conflict of laws.
- XII. **CLAUSE 12: DISPUTE RESOLUTION.** Any controversy, conflict, or claim arising out of or in connection with this contract, including any matter relating to its existence, validity, interpretation, performance, breach, or termination, shall be submitted to arbitration in accordance with the rules of the Arbitration Center of the Lima Chamber of Commerce and shall be finally settled in accordance with the arbitral award issued in the Arbitration Procedure. The place of arbitration shall be in the city of Lima, Peru, and the language of arbitration shall be Spanish.
- XIII. **CLAUSE 13: COMPENSATION.** The parties agree to waive any right to claim or seek any compensation or indemnification in relation to any indirect, special,



incidental, or consequential damages, including, without limitation, loss of profits or income, or the cost of replacement or repair of any equipment, property, or information, arising out of or in connection with this contract. The waiver of these rights does not limit the parties' ability to seek compensation for any direct damages they may suffer.

CONTRACTUAL GUIDELINES 5: Clause s for sustainability consulting companies that act as a service provider for a third party, providing their sustainability reporting services using the Autonomouz Sustainable software.

- I. **CLAUSE 1: CONFIDENTIALITY.** The sustainability consulting company that uses the master modality of Autonomouz Sustainable for managing corporate account portfolios agrees to maintain the confidentiality of the information provided by its clients, including the information contained in the Autonomouz Sustainable software. In addition, it shall ensure that its consultants responsible for each account and other personnel involved in the generation of sustainability reports maintain the confidentiality of the information and use it only for purposes related to the generation of sustainability reports.
- II. **CLAUSE 2: DATA PROTECTION.** The sustainability consulting company undertakes to comply with all applicable laws and regulations on data protection, including the Personal Data Protection Law and the Personal Data Protection Law in the Telecommunications Sector. The sustainability consulting company shall take adequate technical and organizational measures to ensure the security of personal data contained in the Autonomouz Sustainable software and in the generated sustainability reports.
- III. **CLAUSE 3: ACCESS TO SOFTWARE.** FUTURE CONCEPT SAC provides the consulting company with a Master account to access and use the Autonomouz Sustainable software. The consulting company shall ensure that its consultants responsible for each account only access the information necessary for the generation of sustainability reports. Additionally, the consulting company shall ensure that access to the Master account is limited and controlled, and measures are taken to prevent unauthorized access.
- IV. **CLAUSE 4: LIABILITY.** The consulting company shall be responsible to FUTURE CONCEPT SAC and its clients for any breach of the obligations established in the contract and for any damage or harm caused to FUTURE CONCEPT SAC or its clients in relation to the use of the Autonomouz Sustainable software and the generation of sustainability reports.

Lima, October 1st, 2022.



+51 992 743 849



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



innovacion@futurelab.pe

www.futurelab.la

