1. Objective:

The main objective of this document is to establish normative values related to information security for suppliers and contractors for **Colombian Outsourcing Solutions S.A.S (COS),** so that throughout the execution of their tasks they can have access to information, systems information or company resources in general, with the purpose of protecting their confidentiality, integrity and availability of information and systems managed by the company.

Through this, the supplying and contracting companies that these security policies are applied to are responsible of informing people reporting to **Colombian Outsourcing Solutions S.A.S (COS)** of the following, as well as maintaining their commitment to do so in writing that they will respect such policies.

2. Contract with the supplier and/or contractor:

Any supplier and contractor carrying out functions for the company that have access to information, systems information or any general resources for **Colombian Outsourcing Solutions S.A.S (COS)** must:

2.1 Count with their respective suitability verification and will be subject to verification of any documentation and information supplied.

2.2 Count with a contract that is written and signed, in addition, a clause or document will be added in order to guarantee confidentiality.

2.3 The supplier and/or contractor and their employees must know and comply with the information security policies under the terms established by **Colombian Outsourcing Solutions S.A.S (COS).**

2.4 The supplier must give any information necessary to **Colombian Outsourcing Solutions S.A.S (COS)** of all of the employees that will be carrying out contractual activities for them.

2.5 Any incompliance of the policies and contractual agreements or normative terms established by **Colombian Outsourcing Solutions S.A.S (COS)** from the supplier and/or contractor regarding information security will be cause for the termination of the contact and respective judicial proceedings will be carried out in case either happens.

2.6 Management activities and mechanisms established by **Colombian Outsourcing Solutions S.A.S (COS)** that allow the protection of threats that can affect our network and its applications won't be avoided.

2.7 Security aspects will be identified, as well as the levels of service and management mechanisms in order to guarantee the security of our network service provided by suppliers and contractors.

3. Execution of contractual tasks by the Supplier:

3.1 All information related to activities carried out at **Colombian Outsourcing Solutions S.A.S (COS)** will be considered confidential.

3.2 The supplier will fulfill the tasks and obligations applied to the use of systems information according to the norm established by **Colombian Outsourcing Solutions S.A.S (COS).**

3.3 Technology infrastructure will be located in secure areas and protected with the purpose of reducing the risks caused by external threats. It's the supplier's responsibility that this equipment be kept safe in case they are used.

4. **Use of technology infrastructure:**

4.1 All technology infrastructures will be protected against provision failures with the electrical supply, thus the connection of any equipment or electrical and communication circuits must be checked by the technology area, in order to avoid interceptions or damages.

4.2 Previous validation must be solicited and indicated control measures will be implemented throughout the entire technology infrastructure in case any specific needs requires them to be located outside of their protected areas in **Colombian Outsourcing Solutions S.A.S (COS)** or outside of the organization.

4.3 All technical equipment that is property of or administered by **Colombian Outsourcing Solutions S.A.S (COS)** cannot leave the premises without authorization from the IT Director or personnel. This authorization must be done through e-mail or through the Help Desk tool, in compliance with the equipment transfer policies of **Colombian Outsourcing Solutions S.A.S (COS).**

4.4 **Colombian Outsourcing Solutions S.A.S (COS)** will provide, in accordance to the contractual needs, updated operational procedures to the suppliers and/or contractors that need them.

4.5 Any changes regarding technology infrastructure and resources are prohibited, in case any changes need to be made, these need to be approved directly by the General Manager of **Colombian Outsourcing Solutions S.A.S (COS).**

4.6 **Colombian Outsourcing Solutions S.A.S (COS)** will provide the supplier or contractor with areas and/or technology equipment for the execution of the contractual activities.

4.7 In accordance to the criticality and/or risk of the contracted service, any changes in the service provided must be previously validated by **Colombian Outsourcing Solutions S.A.S (COS).**

4.8 Suppliers and contractors are prohibited to use codes that are not authorized. The equipment configuration will allow all authorized code to work in accordance to the norms established.

4.9 Suppliers and contractors are not allowed to take pictures of the technology areas in **Colombian Outsourcing Solutions S.A.S (COS)**, only the IT Director can authorize access to these areas in accordance to contractual terms.

5. Use of extractable units

5.1 The use of extractable information units must be previously validated by the IT Director with the exclusive means of information collection in relation to the contract established.

5.2 When the contractual relationship with the company ends, any extractable information units given to the supplier for the execution of their tasks must be given back.

5.3 The use and storage of information on extractable units and the manipulation of such units will be continuously controlled through the norm established by **Colombian Outsourcing Solutions S.A.S (COS).**

5.4 Access to **Colombian Outsourcing Solutions S.A.S (COS)** documents located in such units or physically is prohibited unless otherwise explicitly stated in writing or presented in the service contract.

5.5 Information exchanges between the service provider and COS will be established depending on the criticality of the task established by **Colombian Outsourcing Solutions S.A.S (COS),** through normative controls, procedures and techniques used in order to protect the exchange of such information.

6. **Information Exchange**

6.1 Information exchange and use of such will be controlled through the corresponding agreement or relationship contract between **Colombian Outsourcing Solutions S.A.S (COS)**, the supplier and/or contractor.

6.2 In cases that the services provided include information transit, normative controls and techniques will be established by the supplier or contractor so that any unauthorized use or destruction of information is avoided. **Colombian Outsourcing Solutions S.A.S (COS)** reserves the right to audit these controls or require the implementation of additional protection.

6.3 COS could require that information transmitted through the use of electronic messaging be adequately protected by the supplier and contractor, requiring the compliance of a specific norm and/or the implementation of auditable technique controls.

6.4 **Colombian Outsourcing Solutions S.A.S (COS)** information transmission to other organizations is prohibited. In case this is needed in order to execute tasks of the contracted service, the service provider must solicit the necessary authorization to **Colombian Outsourcing Solutions S.A.S (COS)** and this information must be added to the contractual agreements of both parties.

6.5 Previous validation must be completed prior to the transmission of information. In accordance to the classification levels and legal requirements established, **Colombian Outsourcing Solutions S.A.S (COS)** will solicit specific security controls and such will be audited.

7. **Supervision**

7.1 Controls used in order to verify the security requirements set up previous to the provision of services will be implemented and maintained by **Colombian Outsourcing Solutions S.A.S (COS).**

7.2 Services provided will be subject to periodical supervision and revision in relation to the type of service. These are also subject to compliance audits.

7.3 **Colombian Outsourcing Solutions S.A.S (COS)** will make use of monitoring elements that will allow the audit of activities and security events of the supplier or contractor in relation to the needs of the organization, making use of these registries throughout the time it's considered necessary with the purpose of being used as evidence and/or access control supervision.

7.4 All information systems used by the supplier or contractor will be supervised and this information will be looked at periodically.

7.5 Administration and operational activities that can be done by the service provider or contractor on information systems will be registered by **Colombian Outsourcing Solutions S.A.S (COS).**

8. Network Access

8.1 The supplier or contractor will only have necessary access to network, application and information resources required for the execution of tasks for the contracted services. Rights to the access of these will be as minimal as possible in accordance to the needs of the work that needs to be done. Control rules and access will be established in accordance to "need to know".

8.2 Suppliers and contractors will be provided with access to required networks with the means of allowing them to complete the contracted service.

8.3 External connections that need to be made by the supplier or contractor to **Colombian Outsourcing Solutions S.A.S (COS)** infrastructure must be previously validated. In accordance to the connection risk analysis, auditable security controls are required.

8.4 Physical and logical access to diagnostic and configuration infrastructure ports at **Colombian Outsourcing Solutions S.A.S (COS)** is prohibited. In any case that this is required in order to complete the service, such access will be registered.

8.5 In relation to the architecture of the segregated network, connections to such must be done in accordance to the concrete needs of connectivity for the provision of the service. Configuration to routes or invalid access is prohibited by **Colombian Outsourcing Solutions S.A.S (COS)** beforehand.

8.6 Information access will be restricted to sole purpose of your need to know in order to carry out the contracted services of each supplier or contractor.

9. Notification and Incidents related to information security:

9.1 The supplier or contractor will be obligated to notify any security incident that happens through the provision of the service. This notification must be made as soon as possible to the IT Director. Additionally, alert and vulnerability supervision elements will be established in order to detect information security incidents.

9.2 Any weak point, related to information security, will be notified through the IT Director. Any suspected weak point in security shouldn't be tried to be proven to exist.

9.3 Omission to notify information security incidents by the supplier or contractor will be treated as a contractual incompliance as well as incompliance to present policies.