Annex XI

Information Security Protocol

Approved by the Administration Board of ACS Servicios, Comunicaciones y Energía, S.A. on 16 December 2020

Translation originally issued in Spanish and prepared in accordance with the regulatory applicable to the Group.

In the event of a discrepancy, the Spanish-language version prevails.

Contents

MODIFICATION CONTROL

VERSION	DATE	APPROVAL BODY	AUTHOR	SUMMARY OF CHANGES
0	December 16, 2020	Board of Directors	Committee for Prevention of Criminal Activities	Initial version

1. Definitions

- **ACS:** ACS, ACTIVIDADES DE CONSTRUCCIÓN Y SERVICIOS, S.A., partner company of the group Grupo ACS.
- **ACS SCE**: ACS SERVICIOS, COMUNICACIONES Y ENERGÍA, S.A., parent company of ACS Industrial.
- **ACS Industrial or the organisation:** ACS Industrial Group. It includes the parent company, ACS SCE, and the several divisions[1] thereof, as well as their respective subsidiaries and temporary joint ventures where the Group companies are involved.
- **CNS**: Security Regulations (CNS in Spanish, set of documents at different levels that make up the requirements, guidelines, and protocols that need to be followed by ACS Group.

2. Introduction

The ACS SCE divisions and their corresponding subsidiaries that make up ACS Industrial adhere to the Information Security Policy approved by the Administration Board of ACS on 14 August 2020. Such Policy seeks for the adoption of the set of measures aimed at preserving the confidentiality, the integrity, and the availability of the information, which constitute the three basic information security components, and whose goal is to establish the requirements to protect the information, the equipment and the technological services that serve as a support for the majority of the business processes of the companies that make up the ACS Group.

1 COBRA GESTIÓN DE INFRAESTRUCTURAS, S.A.U. ("**COBRA**"); CONTROL Y MONTAJES INDUSTRIALES CYMI, S.A. ("**CYMI**"); CYMI BRASIL, S.L.U. ("**CYMI BRASIL**"); DRAGADOS OFFSHORE, S.A. ("**DRAGADOS OFFSHORE**"); ELECTRICIDAD ELEIA, S.L.U. ("**ELEIA**"); ENCLAVAMIENTOS Y SEÑALIZACIÓN FERROVIARIA, S.A.U. ("**ENYSE**"); ELECTRONIC TRAFFIC, S.A. ("**ETRA**"); IMESAPI, S.A. ("**IMESAPI**"); INITEC ENERGÍA, S.A. ("**INITEC**"); INTECSA INGENIERÍA INDUSTRIAL, S.A. ("**INTECSA**"); MAETEL INSTALACIONES Y SERVICIOS, S.A ("**MAETEL**"); MAKIBER, S.A. ("**MAKIBER**"); MANTENIMIENTO Y MONTAJES INDUSTRIALES, S.A. ("**MASA**"); SOCIEDAD ESPAÑOLA DE MONTAJES INDUSTRIALES, S.A. ("**SEMI**"); and SICE TECNOLOGÍAS Y SISTEMAS, S.A. ("**SICE**").

This Information Security Policy is the milestone that regulates the CNS of ACS Group. The CNS shall be implemented by each ACS Industrial division through a set of documents (standards of use, regulating standards, procedures, handbooks, guidebooks, best practices, etc.) in such a way that the cover all aspects, up to the operational procedure level.

Today, information technologies are facing an increasing number of threats, which entails an ongoing effort to adapt and manage the risks introduced by them.

2.1 Purpose

The main purpose of this Protocol is to define the basic principles and rules for the management of information security. The ultimate goal is to achieve for all ACS Industrial divisions to guarantee security information and minimise non-financial risks arising out of an impact caused by an inefficient management of information security.

2.2 Scope

The Protocol shall be applicable to all ACS Industrial divisions, which shall need to comply with this minimum requirement notwithstanding the possibility that they may have more restrictive policies and improve security as much as possible. Additionally, the ACS Industrial divisions shall need to adapt and implement this Protocol in their subsidiaries and they shall report to the parent company of ACS Industrial on their fulfilment of such Protocol, in the execution of monitoring processes of the management system of ACS Industrial's Legal Compliance. The scope of this Protocol covers all information of the ACS Industrial divisions regardless of the manner in which it is processed, who accesses the information, the means that contains the information or the place where it is located, be it printed information or information stored electronically.

The Protocol shall be informed on the corporate website of each division and be available in a shared repository of the relevant division, in such a way that it is accessible by all individuals.

2.3 Adaptation and implementation of the Protocol by the divisions

This Information Security Protocol has been adapted for the application thereof to each of the ACS Industrial divisions. Each division shall decide the manner in which it adapts the Protocol to its operations through specific documents, that is to say, its CNS, which shall always be in line with the guidelines herein.

Consequently, each of the ACS Industrial divisions shall use the Protocol defined herein as a minimum requirement and adapt it to its conditions and way of working, through different types of documents, so as to achieve a definition of the security requirements at an operational level.

3. Principles of the Information Security Protocol

This Protocol is an answer to the recommendations of the best information security practices included in the International Standard ISO/IEC27 001, as well as to the fulfilment of current information in terms of personal data protection and regulations that, within the scope of the information security, may affect ACS Industrial.

Likewise, ACS Industrial establishes the following basic principles as main guidelines in terms of information security that need to be always present in any activity related to the processing of information.

- Strategic scope: The information security shall need to have the commitment and support of all executive levels of the ACS Industrial divisions in such a way that it can be coordinated and integrated with the other strategic initiatives so as to conform a working frame that is fully consistent and efficient.
- Comprehensive Security: The information security shall be understood as a comprehensive procedure made up of technical, human, material and organisational elements, thus avoiding, except for cases or urgency or need, any unusual action or short-term processing. The information security shall be considered as part of normal operation, and it shall be present and applied throughout the process of design, development and maintenance of the information systems.

- Risk Management The risks analysis and management shall be an essential part to the information security process. The risk management shall allow the preservation of a controlled background, minimising the risks down to acceptable levels. The reduction of such levels shall be made through the deployment of security measures, which will establish a balance between the nature of the data and the processing activities, the impact and the probability of risks to which they are exposed and the efficiency and the cost of security measures.
- Proportionality: The establishment of protection, detection, and recovery measures shall be proportional to the possible risks and criticality as well as to the value of the information and the services affected.
- Ongoing Improvement: The security measures shall be reassessed and updated on a regular basis to adequate their efficiency to the constant evolution of the risks and protection systems. The information security shall be tended to, reviewed and audited by qualified personnel.
- Security by default: The systems shall be designed and set in such a way that they guarantee a sufficient level of security by default.

ACS Industrial considers that the functions of information security need to remain integrated at all hierarchical levels of its personnel.

Given that the information security involves all ACS Industrial personnel, this Protocol shall need to be known, understood, and undertaken by the integrity of its employees.

In order to achieve the goals in this Protocol, ACS Industrial shall establish a preventive analysis strategy on risks that may affect it, and shall identify such risks and implement controls to mitigate them. ACS Industrial shall likewise establish regular procedures for reassessment. Throughout this cycle of ongoing improvement, ACS Industrial shall keep the definition both regarding the accepted residual risk level (risk appetite) as well as regarding the tolerance thresholds).

4. Commitment by the Executive Board

The ACS Industrial Executive Board, aware of the importance of the information security to successfully achieve their business goals, undertakes to:

- Promote functions and responsibilities within the scope of the information security in the organisation.
- Provide suitable resources so as to reach the information security goals.
- Encourage the dissemination and awareness-raising of the Information Security Protocol among ACS Industrial's employees.
- Demand compliance with the Protocol, the current legislation, and the requirements by regulators within the scope of information security.
- Consider the information security risks of the information regarding decision-making.

5. Roles and responsibilities

ACS Industrial undertakes to safeguard the security of all assets under their responsibility through the necessary measures, always guaranteeing compliance with the different regulations and laws applicable.

Each ACS Industrial division shall name a person responsible of defining, implementing and monitoring the cybersecurity measures and information security measures. This figure shall need to be established from a governmental or managing background, and they shall be in charge, inter alia, of applying the segregation principles of functions and the maintenance of communications with the authorities and special interest groups in terms of information security.

This figure shall undertake the functions that, generally speaking, are assigned hereby to such a figure.

It shall be their responsibility to develop and preserve the Protocol, ensuring that it is adequate and convenient according to the evolution both of the ACS Industrial division for which they are responsible and the legislation in force.

6. Management of Human Resources Security

The Human Resources department shall need to perform their management pursuant to the security criteria established in the Information Security Protocol, as this is a key point to ensure compliance therewith.

The requirements established in this Protocol shall be safeguarded at all times, including in the phase prior to the hiring, the hiring phase, and the contract termination phase of employees.

6.1 Training and raising awareness

ACS Industrial shall ensure that all personnel receives a suitable level of training and raising of awareness in terms of information security within the periods established under the applicable regulations, namely in terms of confidentiality and prevention of information leaks.

Likewise, employees shall need to be informed on the updates of the security policies and procedures that will affect them as well as on the existing threats, in such a way that compliance with this Protocol can be ensured.

On another note, employees shall be obliged to act diligently with regard to the information, and further ensure that such information does not fall in the hands of unauthorised employees or third parties.

6.2 Clean Desk Policy

The following requirements are established for the purpose of preserving the security at work desks:

- The session shall be blocked in the equipment when the employee leaves their desk, both manually (user blocking) and in an automated way through the screen block setting.
- The working space shall need to be tidied up at the end of the day. This includes the need for all documents or information support to be left out of sight, and to store those classified as confidential or secret under lock (See Annex: Classification Levels)
- The desk shall be kept tidy and free of documents or information supports that may be seen or accessible by other people.

7. Asset Management

Information assets needed for the provision of the business processes of ACS Industrial shall need to be identified and inventoried. Additionally, the asset inventory shall need to be updated.

The classification shall be made of assets according to the type of information to be processed, pursuant to the provisions under paragraph 8. Classification of Information

A Person in Charge shall need to be appointed that shall manage information assets throughout the integrity of the life cycle. The Person in Charge shall keep a formal record of users with an authorised access to such asset.

Likewise, for each asset or information element, a person in charge or owner must exist, who will have the responsibility of ensuring that the asset is inventoried, duly classified and adequately protected.

The settings of the assets shall need to be updated regularly so as to allow the monitoring thereof and ensure a correct update of the information.

7.1 BYOD devices or personal devices management

ACS shall allow the policy known as BYOD (Bring Your Own Device that allows employees to use their own personal resources or mobile devices to access resources or information of the organisation.

Additionally, users shall take into account a series of requirements establishes in this Protocol:

- The same security measures and settings shall need to be applied to the BYOD devices that process information as the remaining of ACS Industrial devices.
- The user shall be responsible for BYOD devices.

- Users shall keep the BYOD device where information of any type pertaining to ACS Industrial is processed updated. Likewise, they shall have security applications (antivirus, antimalware, etc.) installed in order to avoid security breaches.
- Employees shall need to previously notify their Head of Area on the use of BYOD devices.

7.2 Management of the life cycle of the information

ACS Industrial shall need to manage the life cycle of the information adequately, in such a way that incorrect uses in any of the phases are avoided.

The life cycle of an information asset has the following phases:

1. Creation or gathering: this phase involves registers in their point of origin. This could include their creation a member of ACS Industrial or the receipt of information from an outside source. It includes mailing, forms, reports, sketches, entry/exit from computers and other sources.
2. Distribution: it is the management process of the information one it has been created or received. This includes both the internal distribution and the external distribution, as the information leaving ACS Industrial becomes a register of an operation with third parties.
3. Use or access: this is carried out after the information is distributed internally, and it may generate business decisions, new information, or serve other purposes. It details the set of users authorised by ACS Industrial to access the information.
4. Storage: it is the process of organising the information into a predetermined sequence and the creation of a management system to guarantee its utility within ACS Industrial. If a storage method is not established to present the information, its recovery and use would be nearly impossible.

5. Destruction: it establishes the practices for the elimination of the information that has fulfilled all retention periods defined and the information that is no longer useful for ACS Industrial. The preservation periods of the information shall need to be based on regulations, laws or legal requirements that affect ACS Industrial. The business needs shall likewise be taken into account. If none of these requirements demands for the information to be preserved, it needs to be discarded through means that guarantee the confidentiality thereof during the destruction process.

ACS Industrial shall identify the security measures pursuant to this Protocol in order to ensure a correct management of the life cycle of the assets.

7.3 Management of back-up copies

Back-up copies shall need to be performed of the information, the software and the system, and such back-ups shall be verified regularly. For such purpose, back-up copies shall be performed of applications, files, and databases with a weekly periodicity, at least, unless no update has occurred during such period. Where appropriate, a greater frequency of back-up copy performance can be established if the information to be safeguarded has a high impact for ACS Industrial and/or has a high level or transactional nature.

As a general rule, the frequency with which back-up copies shall be performed will be es4tablished according to the sensitivity of the applications or data, pursuant to the information classification criteria declared in the annex “Classification Levels”.

Back-up copies shall need to receive the same security protections as the original data, thus ensuring the correct preservation thereof, as well as adequate access controls.

As a general rule, and provided that this is possible, it shall be required that the information in back-up copies be encrypted. This requirement shall be mandatory for certain types of confidential information.

Restoration tests of the available back-up copies shall be performed as well as of the restoration processes defined, for the purpose of ensuring the correct functioning of the processes. Such tests shall be carried out on a regular basis and be documented.

A preservation period shall be established of the back-up copies up to their destruction once the existence period has expired.

The back-up copies of both master files and applications and information files shall be located at safe places with restricted access. Likewise, support copies shall be preferably located at a centre other than the centre that generated them.

8. Information Classification

In each division, the Person in Charge of the Area shall define a classification model of the information that allows to know and implement the necessary technical and organisational measures to preserve the availability, the confidentiality, and the integrity thereof. The classification model shall need to include the requirements and the conditions established in this paragraph of the Protocol.

The Person in Charge of the Area of each division shall be responsible for the update thereof when deemed appropriate, as well as for disseminating the classification model among the employees within their scope of action.

8.1 Type of information

ACS Industrial shall classify the information according to the support where it is being used.

a) Logical supports: information that is being used through IT means, electronic mail, or information systems developed in a tailored manner or acquired from a third party.

b) Physical supports: information that is on paper, magnetic supports such as USBs, DVDs, etc.

8.2 Classification Levels

Depending on the sensitivity of the information, ACS Industrial shall catalogue the information on five levels, see the precise definition in the Annex “Classification Levels”:

- Public use
- Limited dissemination
- Confidential information
- Reserved information
- Secret information

8.3 Management of privileged information

Information that is considered reserved, confidential, or secret shall need to be processed carefully. Extraordinary or additional security measures shall need to be defined for the due processing of privileged information. This type of information shall be submitted encrypted and through safe protocols.

8.4 Labelling of the information

ACS Industrial shall perform a labelling through manual or, to the extent possible, through automated means to allow a suitable processing of the security measures applied in each case.

The documents or the materials shall be labelled, such as annexes, copies, translations or extracts thereof, according to the information classification levels defined above, except for the information considered “of public use”.

A process or procedure shall be defined for the labelling of the information pursuant to the following requirements:

- Ensuring that the labelling of the information reflects the diagram adopted on information classification.
- Ensuring that labels are easily recognisable among all employees.
- Provide orientation to employees on where and how to set or use the labels, according to the information access process or access to the assets that support it.
- State the exceptions where labelling can be omitted without such an omission being a breach of the duty to classify the information.

Special attention shall be paid and the utmost care shall be provided to the labelling of physical assets containing reserved information or secret information, in order to avoid thefts and be easily identifiable.

The technical measures shall need to be established, if needed be, as well as viable automatic labelling measures of the information stored in digital media.

ACS Industrial shall ensure the training of all its employees in information labelling, as well as the specific training of employees who process reserved or secret information.

8.5 Handling of information

ACS Industrial shall be in charge of developing and implementing a set of procedures that is adequate for the de handling of information. Measures shall be adopted needed to protect the information pursuant to its classification.

Confidential information or secret information shall at all times be guarded throughout the life cycle of such information.

8.6 Privacy of the information

ACS Industrial shall guarantee the privacy of personal data for the purpose of protecting fundamental rights of natural persons, namely their right to freedom from injury to honour, personal and family life privacy, and self-image, by implementing measures to regulate the processing of data.

ACS Industrial shall need to comply with current legislation in terms of personal data protection according to the jurisdiction where it is established and operating (by way of an example, Organic Act 3/2018 of 5 December, on Data Protection an Digital Rights Guarantees for the case of Spain) and shall need to include the necessary measures to comply with the regulations.

The necessary measures shall need to be implemented to ensure the privacy of the information through all the phases of its life cycle (pursuant to paragraph 7.2 *Management of the life cycle of the information*).

9. Prevention of information leaks

The leak of information is the uncontrolled exit of information (either intentional or unintentional) that causes for such information to reach unauthorised persons or for the owner thereof to lose control over the access to it by third parties.

The information leak vectors shall need to be analysed according to the conditions and the work operation of each ACS Industrial division. To that end, the assets whose leak entails a greater risk for each company need to be identified, based on the criticality of the asset and the classification level of the information. In addition, the possible ways of theft, loss or leak of each of the assets throughout their different life cycles need to be identified.

ACS Industrial shall define procedures to avoid the occurrence of situations that may entail the loss of information, as well as action procedures in case a communication is made of an information leak.

Training shall need to be ensured of all employees on best practices in order to prevent information leaks. Especially, at least the following aspects need to be taken into account:

- Process of handling of high-criticality devices.
- Suitable use of removable devices such as USBs, CD/DVDs or similar.
- Use of Email
- Verbal transfer of information
- Document printing
- Document exit
- Use of mobile devices
- Use of the Internet
- Clean and tidy desks (see paragraph 6.2 Clean Desk Policy).
- Neglected equipment

10. Access control

All information systems of ACS Industrial shall need to have an access control system to access them. Likewise, the access control focuses on ensuring access to users and preventing unauthorised access to information systems, including measures such as protection through passwords.

Access control shall be understood both from a logical perspective (oriented towards information systems) and from a physical perspective (see paragraph 12 Physical Security and Background Security).

10.1 Business requirements for access control

ACS Industrial shall undertake a series of business requirements for access control. Inter alia, at least:

- There will only be sole users that shall not be shared. Likewise, privileges of users shall be initially assigned through the principle of minimum privilege.
- Generic users shall be forbidden. Failing that, user accounts associated to the nominative identity of the associated person shall be used.

10.2 Rights of Access

ACS Industrial shall implement access controls that guarantee that users are only awarded the necessary privileges and rights to carry out their tasks.

Rights of access shall need to be established depending on:

- Access control based on roles: profiles or roles of access shall be established per application and/or system to assign such profiles or roles of access to the different users.
- Need to know: Access shall only be granted to a resource when there is a legitimate need for the performance of the activity.
- Minimum privileges: the permits granted to users shall be the minimum.
- Function segregation: a correct segregation of functions needs to be ensured to implement and assign rights of access.

Likewise, no user shall be able to access a controlled information system on their own without the approval of the Person in Charge of the own user (or the designated person).

10.3 Logical Access Control

ACS Industrial shall establish an adequate password policy in line with the best practices on security. The password policy shall define the password requirements and the preservation periods of one password.

The password policy shall be known by all ACS Industrial employees.

10.4 Telecommuting

Remote access to the network by the ACS Industrial divisions through telecommuting, that is, from outside the facilities owned, shall need to be controlled.

The services of remote connection to work shall be exclusively limited to ACS Industrial personnel. Any use thereof by any other collaborator shall request an authorisation by the Head of Security.

The equipment used for the connection under the modality of remote work may be the property of the employee or provided by ACS Industrial. In any event, it is compulsory for the equipment to meet the following security criteria:

a) Ability to perform a connection through a VPN.

b) Include an operational system updated with the last security patches and updates.

c) Antivirus software installed.

d) Personal firewall software installed.

Telecommuting from the employee's own device shall request for all relevant security measures so that remote working does not entail a threat against the security of the ACS Industrial information. In addition, additional security measures to those in place may be established to ensure a safe remote connection in a more reliable manner.

The telecommuting service shall be monitored and controlled with a registration of both the connection and the activity pursuant to the security protocols.

11. Management of the life cycle of the identity

The ACS Industrial divisions shall define and implement an adequate management system of the life cycle of the identity. An identity is the set of features that univocally identify every person with a physical or logical access to the information systems of ACS Industrial. The life cycle of the identity is the process followed by the user identity since the creation thereof up to the suppression thereof.

The life cycle of an identity has the following activities:

a) Creation and assignation of identity

b) Periodical review

c) Modification or suppression

The management of this cycle requests for a definition of the security requirements and responsibilities of each of the stages, for the purpose of centralising and enabling the management processes associated to them.

The life cycle management of the identity shall be in line with the HR Department with the purpose of verifying the identities according to the registrations and de-registrations of employees and their communications in the information systems.

11.1 Privileged Identities

The assignment and the use of privileged rights of access shall be restricted and controlled. This privileged access is the access to systems as an administrator or with a role that offers the possibility to modify the settings of the system.

The assignment of privileged rights of access shall be controlled through a formal authorisation process pursuant to the access control policies. At least the following requirements shall be considered:

- The privileged rights of access associated to each system or process shall be identified (for example, operating system, data base management system or application management system), as well as the users to which these shall be assigned.
- The assignment of privileged rights of access shall be carried out pursuant to the needs of use, based on the minimum privilege and the need to know.

- An authorisation process that includes a record of the privileges assigned shall be defined. Privileged rights of access shall not be assigned until the authorisation process is complete.
- The requirements for the expiration of the privileged rights of access shall be defined.
- The skills of the users with privileged rights of access shall be reviewed on a regular basis for the purpose of verifying if they are in line with their obligations.
- Specific procedures and mechanisms shall be established and maintained to avoid an unauthorised use of generic administration user accounts, pursuant to the setting capacities of the systems.
- Procedures and mechanisms shall be established that ensure the confidentiality of secret authentication information for generic administration users (for example, frequent modification of a password, mechanisms of secure password sharing, etc).

12. Physical Security and Background Security

Physical spaces where ACS Industrial information systems are located shall be duly protected through perimeter access controls, surveillance systems and preventive measures so that Security incidents may be avoided or mitigated (unauthorised accesses to information systems, thefts or sabotages) as well as environment accidents (fires, floods, outputs, etc.).

In addition, the Person in Charge of the Area of each division shall need to guarantee that an information access control is in place for information that is in a physical format through a register that records who accesses the information. On another note, the confidential information shall be stores with the specific measures like fire-proof wardrobes.

13. Cloud computing security

ACS Industrial shall keep a policy of cloud computing security that establishes the adequate security measures for the confidentiality, the integrity and the availability of the information. Depending on the type of service model in the cloud, different security measures shall need to be applied.

- Infrastructure: first, it shall be ensured that the Provider monitors the background so as to detect unauthorised changes. In addition, strong authentication and access control levels shall need to be established for the administrators and the operations carried out by them. Last, the installations and/or settings of shared elements shall be registered and connected for the purpose of obtaining a suitable traceability.
- Platform: additionally to the measures stated in the infrastructure service model, the Provider of the service shall provide security mechanisms corresponding to the life cycle of the secure software, pursuant to paragraph 15. Security in the life cycle of the system development.
- Software: additionally to the measures states in the service model of the Platform, ACS Industrial and the Provider shall follow OWASP (Open Web Application Security) as a guidebook for security in applications.

14. Operational security

All ACS Industrial information systems that process or store information owned by them shall need to have the relevant security measures that optimise their suitable maturity level (monitoring, change control, reviews, etc.). Likewise, networks shall be managed, controlled and monitored suitably, for the purpose of protecting them from threats and maintaining the security of the systems and applications that use the network, including access controls to the network, thus protecting all the information transferred through these elements and/or backgrounds.

15. Security in telecommunications

The network architecture of ACS Industrial shall need to have prevention, detection and response measures to avoid breaches in the internal and external domains. “Internal domain” shall be understood as the local network composed of the technological elements of ACS Industrial exclusively accessible from the internal network. On another note, “external domain” shall be the network accessible from outside the ACS Industrial network.

It is very important to administer the security of the networks that cross the ACS Industrial perimeter through the implementation of additional controls for sensitive data that circulate through the public communication networks.

For this reason, ACS Industrial shall define security guidelines to be followed regarding the transfer of information, as well as the security measures in the use of portable devices, Internet services and mailing services, as well as specific controls that allow for a secure connection to the ACS Industrial security systems from outside its facilities.

16. Security in the life cycle of the system development

All purchase, implementation and maintenance of the systems shall have some minimum security requirements for the development of software, the systems and the data in line with the sector's best practices. In addition, the management of the trials, the monitoring of the changes and the inventory of the software shall need to be performed.

Each department of the ACS Industrial division shall need to take into account information security in all their system processes and data processes, selection procedures, development and implementation of applications, products and services.

17. Security in the Providers

Special attention needs to be paid at the time to assess the criticality of all services that are prone to be subcontracted in a way that those that are relevant from an information security point of view can be identified, either because of their nature, because of the sensitivity of the data that need to be processed or because of the dependence on the business continuity.

With regard to the providers of these services, selection processes shall need to be treated carefully, together with contractual requirements such as contract terminations, the monitoring of the levels of service, the return of data and the security measures implemented by such a provided, which shall be, at least, equivalent to the measures established in this Protocol.

18. Incident Management

All ACS Industrial employees have the obligation and the responsibility to identify and notify any incident or crime that may compromise the security of their information assets through a notification to the Head of Security of the relevant division. Likewise, ACS Industrial shall implement procedures for the due handling of the incidents detected.

A response management procedure in case of incidents shall need to be defined where an incident categorisation process is established, together with an impact analysis on business and scalation by the information security and cybersecurity function vis-à-vis any incident related to information security.

19. Business continuity

As a response to quality requirements and best practices requirements, ACS Industrial shall make available a Business Continuity Plan as part of its strategy to guarantee the continuity in the provision of essential or critical services and the due handling of the impacts on business vis-à-vis possible scenarios of crisis, and shall provide a reference framework so that the company may act pursuant to it if needed be. This Continuity Plan shall need to be updated and tested on a regular basis. Likewise, a Recovery Plan for Disasters shall be defined and maintained in line with the business continuity. Such a plan shall cover the continuity of the functioning of the information and communication technologies.

ACS Industrial shall be in charge of the training of all ACS Industrial employees in terms of Business Continuity. Training in terms of Business Continuity shall be reviewed periodically so that such training is always fully in line with the existing Plan.

20. Legal Compliance

ACS Industrial shall undertake to provide the necessary resources to comply with all legislation and regulations applicable to its activity in terms of information security and it shall further establish a responsibility of compliance on all its members. In this regard, compliance with all legislation, standards or regulations applicable shall be ensured.

21. Handling of Exceptions

Any exception to this Information Security Protocol shall be registered and notified to the Head of Information Security of the relevant ACS Industrial division. These exceptions shall be analysed to assess the risk they could introduce in the company and, based on the categorisation of these risks, they shall be undertaken by the person requesting the exception together with the Persons in Charge of the business.

22. Disciplinary sanctions

Any breach of this Information Security Protocol may result in the adoption of disciplinary actions pursuant to the internal procedure of each ACS Industrial division. It is the responsibility of all employees in ACS Industrial to notify the Head of Information Security of the company affected by any event that may entail a breach of any of the guidelines provided for in this Protocol.

23. Protocol Review

The approval of this Protocol implies that the implementation thereof shall have the support of the Executive Board so as to reach the goals established therein, as well as to comply with all the requirements thereof.

This Information Security Protocol shall be reviewed and approved by the Administration Board from time to time. Notwithstanding the above, if relevant changes were to occur for the company or significant changes were to be identified in terms of threats and risks, be they operational, legal, regulatory or contractual, it shall be revised provided this is deemed necessary, thus ensuring that the Protocol remains adapted to ACS Industrial's reality at all times.

24. Annexes

24.1 Annex: Classification Levels

Level	Level Detail	Examples
Public use	This is information that may be known by any type of person and whose fraudulent use does not entail a risk for the interests of ACS Industrial.	Product catalogues and information available on the corporate webpage of each division are examples of this type of information.
Limited dissemination	This information is used by the ACS Industrial areas and if used fraudulently, this entails a risk for the interests of ACS Industrial that is not very significant.	Emails and work documents of the ACS Industrial areas are examples of this type of information.
Confidential Information	Information that may only be known by a reduced number of people and whose fraudulent use may have a significant impact on the interests of ACS Industrial.	Audit reports and strategy reports of ACS Industrial are examples of this type of information.
Reserved information	Information that only the owner thereof as well as, in certain cases, a limited group of people may know. An unauthorised communication or dissemination of this type of information may seriously harm the interests of ACS Industrial.	Some examples of this type of information are communications between executive members or shareholders containing relevant decisions for the operation of the business.
Secret information	Information that may solely be known by the owner thereof and under no circumstance revealed. An unauthorised communication or dissemination of this type of information may cause exceptionally serious damages to the interests of ACS Industrial.	Some examples of this type of information are access codes of collaborators, client credentials or cryptographic codes to access systems.