Information Security Policy

Reference	31_Política de Seguridad de la Información_2_2021_ENG
Title of Standard	Information Security Policy
Geographical scope	Worldwide
Category	Policy
Approval date	July 27 2021
Approval body	Board of Directors
Current version	V2

Important information about this document	
Document identification	Information Security Policy
Reference	31_ Information Security Policy_2_2021
Geographical scope of application	Worldwide
Section on other rules it develops	
Rules that it replaces	Information Security Document
Rules that it repeals	Information Security Document
Main staff responsible for its surveillance	Audit Committee and Compliance Committee
Proposing body or department	Audit Committee
Author	CISO
Approval body	Board of Directors
Date of approval of the current text	July 27 2021
Date of application	July 27 2021
Published and accessible on	Extranet and Intranet

Version	Date	Approval body	Author	Summary of changes
V1	August 14, 2020	Board of Directors	Compliance Committee	
V2	July 27 2021	Board of Directors	CISO	New paragraph 20 on Security Audits and Vulnerability Management

INFORMATION SECURITY POLICY

1. Introduction

The Information Security Policy (hereinafter, the Policy) seeks to adopt a set of measures to preserve the confidentiality, integrity and availability of information, which are the three basic components of information security, and its objective is to establish the requirements to protect the information, equipment and technological services that support most of the ACS business processes, Actividades de Construcción y Servicios, S.A. (hereinafter, ACS) and the companies that make up its group (hereinafter, the ACS Group).

This Information Security Policy is the cornerstone of the ACS Group's Security Standards Documentation. The Security Standards Documentation (hereinafter, SSD) is a set of documents at different levels that set out the requirements, guidelines and protocols that the ACS Group must follow in terms of security. The SSD shall be developed by each ACS Group company through a set of documents (usage standards, regulatory standards, procedures, manuals, guides, best practices, etc.) in such a way that they cover all aspects presented in the Policy, reaching an operations process level.

Today, information technologies face a growing number of threats, requiring a constant effort to adapt and manage the risks that they cause.

1.1. Objective

The main objective of this high-level Policy is to define the basic principles and rules for information security management. The ultimate aim is to ensure that the ACS Group companies guarantee information security and minimize risks of a non-financial nature resulting from any impact caused by ineffective information management.

1.2. Scope

The Policy applies to the whole ACS Group, which must meet this minimum requirement, without prejudice to more restrictive policies and improve security as much as possible. In addition, the subsidiaries must adapt and develop this Policy in their companies, and report to the ACS Group's parent company on their compliance with this Policy, in execution of the monitoring processes of the ACS Group's Compliance Management System. The scope of this Policy covers all the information of the ACS Group companies, regardless of the way in which it is processed, who accesses it, the medium on which it is held or the place in which it is located, whether it is printed or electronically stored information.

The Policy must be available on the ACS corporate website www.grupoacs.com and in a common ACS repository, so that it is accessible to all persons in the ACS Group.

1.3. Adaptation and development of the Policy by subsidiaries

This Information Security Policy shall be adapted and developed by each of the ACS Group companies. Each company shall decide how it adapts the Policy to its operations by means of specific documentation (its Security Standards Documentation, SSD), which shall always be aligned with the guidelines set out in this document.

Accordingly, each of the companies that make up the ACS Group must use the Policy set out in this document as a minimum requirement and adapt it to its working conditions and methods, through different types of documentation, in order to ensure that security requirements are set down at the operational level.

2. Information Policy Principles

This Policy is in response to the recommendations of the Information Security Best Practices contained in the International Standard ISO/IEC 27001, and complies with the legislation in force regarding the protection of personal data and the regulations that may impact the ACS Group in the field of Information Security.

Additionally, the ACS Group sets out the following basic principles as core information security guidelines that must always be present in any activity related to the processing of information:

- Strategic scope: Information security should be committed to and supported by all management levels of the ACS Group companies so that it can be coordinated and integrated with all other strategic initiatives to form a completely coherent and effective framework.
- Integral security: Information security must be understood as an integral process consisting in technical, human, material and organizational factors, and any ad hoc action or context-specific handling is to be avoided, except in emergencies or where necessary. Information security should be considered as part of the normal operations, present within and applied throughout the process of designing, developing and maintaining information systems.
- Risk management: Risk analysis and management shall form an essential part of the information security process. Risk management shall enable the maintenance of a controlled environment, minimizing risks to acceptable levels. The reduction of these levels shall be achieved through the deployment of safety measures, which shall balance the nature of the data and the way in which it is processed, the impact and likelihood of the risks to which data is exposed, and the effectiveness and cost of security measures.
- Proportionality: The establishment of protection, detection and recovery measures should be proportional to potential risks and to the criticality and value of the information and services involved.
- Continuous improvement: Security measures shall be periodically reassessed and updated to adapt their effectiveness to the constant evolution of risks and of protection systems. Information security shall be monitored, reviewed and audited by qualified personnel.
- Default security: Systems must be designed and configured to ensure a sufficient degree of security by default.

The ACS Group takes the view that Information Security functions should be integrated at every hierarchical level of its workforce.

Since Information Security is the responsibility of all the ACS Group personnel, this Policy must be made known to, understood and taken on board by all employees.

In order to achieve the objectives of this Policy, the ACS Group shall establish a preventive strategy for analysis of the risks that may affect it, identifying them, implementing controls to mitigate them and setting in place procedures to reassess them on a regular basis. In the course of this continuous improvement cycle, the ACS Group shall maintain its definition of both the accepted residual risk level (risk appetite) and its tolerance thresholds.

3. Management Commitment

The ACS Group Management, aware of the importance of information security for the successful execution of its business objectives, is committed to:

- Promoting roles and responsibilities in the field of information security within the organization.
- Providing adequate resources to achieve information security objectives.
- Promoting dissemination and awareness of the Information Security Policy among the ACS Group employees.
- Requiring compliance with the Policy, current legislation and regulatory requirements on information security.
- Considering information security risks in decision-making.

4. Roles and responsibilities

The ACS Group is committed to ensuring the security of all assets under its responsibility through the necessary measures, ensuring compliance with the various applicable laws and regulations.

Both ACS and each subsidiary of the ACS Group shall appoint a person responsible for defining, implementing and monitoring cybersecurity and information security measures. This figure should be taken from a governance and management environment, and shall have among their duties and responsibilities the application of principles of separation of duties and contact with authorities and special interest groups in information security.

The figure shall carry out the duties generally attributed by this Information Security Policy.

It shall be their responsibility to develop and maintain the Policy, ensuring that it is appropriate and timely as the ACS Group company for which they are responsible and current regulation evolve.

5. Human Resources Security Management

The Human Resources Department should be managed taking into account the security criteria set out in the Information Security Policy, which is a key factor in ensuring compliance.

The requirements set out in this Policy shall be complied with at all times, including during pre-recruitment, recruitment and upon termination/expiry of employees' contracts.

5.1. Training and Awareness

The ACS Group shall ensure that all personnel receive an adequate level of information security training and awareness within the time limits required by the current regulations, especially in the areas of confidentiality and the prevention of information leaks.

Employees must also be informed of any updates to the security policies and procedures by which they are impacted and of any existing threats, so that compliance with this Policy can be ensured.

Also, employees have an obligation to act diligently with respect to information, ensuring that it does not fall into the hands of unauthorized employees or third parties.

5.2. Clean Desk Policy

A Clean Desk Policy must be complied with by the Company and all employees. The following requirements are in effect for the purpose of maintaining security at the workplace:

- Employees must log out of their computers when leaving their workstations, either manually (user lock) or automatically through the screen lock settings.
- The working environment must be left tidy at the end of the day. This includes the requirement that any documents or information media be kept out of sight, keeping those classified as confidential or secret under lock and key (see Annex: Classification levels).
- The workstation should be kept tidy and free of documents or information media that may be seen or accessed by other persons.

6. Asset Management

The information assets necessary for the provision of the ACS Group business processes must be identified and inventoried. Additionally, the asset inventory should be kept up to date.

Assets must be classified according to the type of information processed, in accordance with section *7. Classification of information*.

A manager must be assigned to perform self-management of information assets throughout the lifecycle. The manager must maintain a formal record of users with authorized access to that asset.

In addition, for each asset or information item, there must be a manager or owner, who shall be responsible for ensuring that the asset is properly inventoried, classified and protected.

Asset configurations should be updated periodically to allow asset monitoring and to facilitate the successful updating of information.

6.1. Manage BYOD devices or personal devices

The ACS Group shall permit a policy known as BYOD (Bring Your Own Device), which allows employees to use their resources or personal mobile devices to access the ACS Group information or resources.

Users must take into account a number of requirements set out in this Policy:

- The same security settings and measures should be applied to BYOD devices that process information as other devices in the ACS Group.
- Users shall be responsible for their own BYOD devices.
- Users must keep their personal BYOD devices up to date if they handle any ACS Group information. They must also have security applications (anti-virus, anti-malware, etc.) installed to avoid security breaches on those devices.
- Employees must be authorized by their Manager to use BYOD devices.

6.2. Information lifecycle management

The ACS Group must properly manage the information lifecycle so that incorrect uses can be avoided during all of the phases.

The lifecycle of an information asset consists of the following phases:

1. Creation or collection: this phase deals with records at their point of origin. This could include their creation by a member of the ACS Group or the receipt of information from an external source. This includes correspondences, forms, reports, drawings, computer input/output or other sources.
2. Distribution: this is the process of managing information once it has been created or received. This includes both internal and external distribution, as the information leaving the ACS Group becomes a record of a transaction with third parties.
3. Use or access: occurs after information is distributed internally and can generate business decisions, generate new information or serve other purposes. It also includes the set of users authorized by the ACS Group to access the information.
4. Storage: this is the process of organizing the information in a predetermined sequence and creating a management system to ensure its usefulness within the ACS Group. Failure to establish a storage method for the presentation of information would make it almost impossible to retrieve and use it.
5. Destruction: sets out practices for the removal of information that has met the defined retention periods and information that is no longer useful to the ACS Group. Retention periods must be based on the requirements of standards and on legal and court requirements applicable to the ACS Group. Business needs should also be taken into account. If none of these requirements necessitate retention of the information, it must be disposed of in ways that guarantee confidentiality during the destruction process.

The ACS Group shall identify security measures in accordance with this Policy to ensure proper asset lifecycle management.

6.3. Management of backup copies

Backup copies of information, software and operating systems must be made and periodically checked. Accordingly, applications, files and databases must be backed up on a weekly basis, at least, unless no updates have occurred during this period. Where appropriate, a higher backup frequency may be imposed if the information to be safeguarded is of high impact to the ACS Group and/or is highly transactional in nature.

As a general rule, the frequency of backups shall be determined based on the sensitivity of applications or data, according to the criteria for classification of information set out in the annex “Classification Levels.”

Backups should receive the same security protections as the original data, ensuring proper retention and access controls.

As a general rule and whenever possible, information in backups should be required to be encrypted. This requirement shall be mandatory for certain types of confidential information.

Restoration tests of available backups and defined restoration processes should be performed to ensure proper functioning of the processes. These must be carried out on a regular basis and documented.

A retention period for backups must be established until they are destroyed after the lifetime has expired.

Backups of master files and application and information files should be placed in secure locations with restricted access. Also, backups should preferably be located at a site other than the one at which they were generated.

7. Classification of information

A data classification model must be created to ensure awareness and implementation of the technical and organizational measures necessary to maintain its availability, confidentiality and integrity. The classification model shall incorporate the requirements and conditions set out in this section of the Policy.

The classification model shall have a person responsible for updating it when deemed appropriate, and for making the classification model known to all employees of the ACS Group.

7.1. Types of information

The ACS Group shall classify the information according to the media on which it is being used:

a) Logical Media: Information that is being used via office media, email or information systems that are custom-developed or acquired from a third party.
b) Physical media: information on paper or magnetic media such as USBs, DVDs, etc.

7.2. Classification levels

Depending on the sensitivity of the information, the ACS Group should catalog the information at five levels. See the precise breakdown in the Annex “Classification Levels”:

- Public use
- Limited distribution
- Confidential information
- Undisclosed information
- Secret information

7.3. Management of privileged information

Information that is considered undisclosed, confidential or secret must be treated with special care. Extraordinary or additional security measures should be set in place for the proper handling of privileged information. This type of information must be sent encrypted and using secure protocols.

7.4. Labeling of information

The ACS Group shall label information using manual or, to the extent possible, automated methods to facilitate proper implementation of the security measures applied in each case.

The documents or materials, as well as the annexes, copies, translations or extracts thereof must be labeled according to the information classification levels defined in the preceding sub-section, except for information considered to be for "public use".

A process or procedure for labeling information must be formulated in line with the following requirements:

- Ensure that the labeling of information reflects the information classification scheme adopted.
- Ensure labels are easily recognizable to all employees.
- Guide employees on where and how labels shall be placed or used, depending on the process of accessing the information or the assets in which it is contained.
- Indicate the exceptions in which labeling may be omitted without prejudice to the duty to classify the information.

Particular attention must be given to the labeling of physical assets containing confidential or secret information and the utmost care taken when labeling such assets to avoid theft, since they are easily identifiable.

Technical measures must be set in place, if necessary and where feasible, for the automatic labeling of information stored on digital media.

The ACS Group shall ensure that all its employees are trained and made competent in the labeling of information, and specifically those employees processing undisclosed or confidential information.

7.5. Handling of information

The ACS Group shall be responsible for developing and implementing an appropriate set of procedures for the correct handling of information. The necessary measures must be taken to protect the information according to its classification.

A chain of custody shall be maintained for confidential or secret information throughout the lifecycle of the information.

7.6. Privacy of information

The ACS Group shall ensure the privacy of personal data in order to protect the fundamental rights of natural persons, especially their right to honor, personal and family privacy and one's own image, by setting in place measures to regulate data processing. The ACS Group shall comply with legislation in force on the protection of personal data in accordance with the jurisdiction in which it is established and operates (for illustrative purposes, the Spanish Organic Law 3/2018, of December 5, on Data Protection and Guarantee of Digital Rights) and must include the necessary measures to comply with the legislation.

Appropriate measures must be implemented to ensure the privacy of information at all stages of its lifecycle (in accordance with section *6.2. Information Lifecycle Management*).

8. Prevention of information leaks

Information leakage is an uncontrolled output of information (intentional or unintentional) that causes the information to reach unauthorized persons or the owner to lose control over accesses made by third parties.

Information leakage vectors must be studied, specific to the working conditions and operations of each company in the ACS Group. Accordingly, those assets whose leakage poses the greatest risk to each company must be identified, based on the criticality of the asset and the level of classification ascribed to the information. In addition, the potential routes of theft, loss or leakage of each asset must be identified in its different lifecycle states.

The ACS Group shall set in place procedures to prevent the occurrence of situations that may cause the loss of information, and procedures to follow in the event of a reported information leak.

Training and competence-building for all employees concerning best practices for the prevention of information leaks must be provided. In particular, at least the following points should be taken into account:

- Process for handling known high-criticality devices
- Suitable use of removable media, such as USBs, CDs/DVDs or similar
- Use of email
- Oral transmission of information
- Printing of documents
- Document output
- Use of mobile devices
- Internet use
- Clean and tidy desks (see section *5.2. Clean Desk Policy*)
- Unattended computers

9. Access control

All ACS Group information systems must have a system for controlling access to them. Access control also focuses on providing user access and preventing unauthorized access to information systems, including measures such as password protection.

Access control shall be understood from both a logical (information systems-focused) and a physical perspective (see section *11. Physical and Environmental Security*).

9.1. Business requirements for access control

The ACS Group shall implement a number of business requirements for access control, which shall be at least the following:

- Usernames must be unique and cannot be shared. In addition, user privileges shall be initially assigned by the principle of least privilege.
- The use of generic usernames must be prohibited. Instead, user accounts associated with the nominal identity of the associated individual are to be used.

9.2. Access rights

The ACS Group shall implement access controls that ensure that users are granted only those privileges and rights that are necessary to perform their functions.

Access rights shall be granted on the basis of:

- Role-based access control: Access profiles or roles must be established for each application and/or system to be able to assign them to different users.
- Need to know: Access to a resource shall only be allowed when there is a legitimate need for the activity to be carried out.
- Minimum privileges: The permissions granted to users should be minimal.
- Segregation of duties: Ensure proper segregation of duties when creating and assigning access rights.

Additionally, it must not be possible for any user to access a controlled information system on their own without the approval of the user's manager (or designated person).

9.3. Logical access control

The ACS Group shall establish an appropriate Password Policy aligned with security best practices. The password policy shall set out password requirements and the length of time the same password can be used.

The Password Policy must be known to all employees of the ACS Group.

9.4. Remote working

Access to the ACS Group network must be controlled when working remotely (from outside the network).

Remote working connection services shall be exclusively for the ACS Group personnel. Use by any other contributor shall require authorization by the Security Officer.

The device used for connection in remote working mode may be owned by the employee or provided by the ACS Group. In any case, it is mandatory for the device to comply with the following security requirements:

a) Ability to connect via a VPN.
b) Have an up-to-date operating system with the latest security patches and updates.
c) Anti-virus software installed.
d) Personal firewall software installed.

Remote working from a worker's own device must be secured using all appropriate security measures, so that remote working does not pose a threat to the information security of the ACS Group. Also, additional security measures may be set in place to provide a more reliable secure remote connection.

The remote working service shall be monitored and controlled, recording both connection and activity in accordance with the security protocols.

10. Identity lifecycle management

The ACS Group companies must create and implement an appropriate identity lifecycle management system. Identity is the set of characteristics that uniquely identify any person with

physical or logical access to the ACS Group information systems. The identity lifecycle is the process that follows a user's identity from creation to deletion.

The identity lifecycle consists of the following activities:

a) Creating and assigning an identity
b) Periodic review
c) Modification or deletion

Managing this cycle requires the setting of stage-specific security requirements and responsibilities, with the aim of centralizing and facilitating the associated management processes.

Identity lifecycle management must be coordinated with the HR Department to verify identity in relation to the incorporation and exit of employees, and to ensure that information systems reflect such changes.

10.1. Privileged identities

The assignment and use of privileged access rights must be restricted and controlled. Privileged access is access to systems as an administrator or with a role that provides the ability to modify system settings.

The assignment of privileged access rights must be controlled through a formal authorization process in accordance with access control policies. At least the following requirements must be considered:

- The privileged access rights associated with each system or process (for example, operating system, database management system or application) and the users to whom they should be assigned must be identified.
- The assignment of privileged access rights should be based on use requirements, based on minimum privilege and need-to-know.
- An authorization process must be set in place that includes a record of the privileges assigned. Privileged access rights must not be granted until the authorization process is completed.
- Requirements upon expiry of privileged access rights must be determined.
- The competencies of users with privileged access rights should be reviewed regularly, in order to verify that they are in line with their obligations.
- Specific procedures and mechanisms must be established and maintained to prevent the unauthorized use of generic user accounts for administration purposes, in compliance with the configuration capabilities of the systems.
- Procedures and mechanisms should be established to safeguard the confidentiality of secret authentication information for generic admin users (e.g. frequent password modification, secure password sharing mechanisms, etc.).

11. Physical and environmental security

The physical spaces in which the ACS Group information systems are located shall be adequately protected by perimeter access controls, surveillance systems and preventive measures, so that the impact of security incidents can be avoided or mitigated (unauthorized access to information systems, theft or sabotage) and environmental accidents (fires, floods, power outages, etc.).

In addition, physical access to information in physical format must be controlled using a paper record of who accesses the information. Also, confidential information must be stored under specific conditions such as fire-proof cabinets.

12. Security when working on the Cloud

The ACS Group shall maintain a Cloud or Cloud computing policy that establishes appropriate security measures for information confidentiality, integrity and availability. Depending on the type of Cloud service model, different security measures must be applied:

- Infrastructure: Several important points must be established for infrastructure services. First, it is necessary to ensure that the service provider monitors the environment for unauthorized changes. In addition, strong levels of authentication and access control must be defined for administrators and the operations they perform. Finally, installations and/or configurations of shared resources must be registered and connected, in order to ensure proper traceability.
- Platform: For platform services, the service must provide appropriate security mechanisms within the secure software developments life cycle, in line with Section 15. *Security in the systems development lifecycle*.
- Software: For software services, the ACS Group and the Cloud service provider shall follow OWASP (Open Web Application Security) as a guide for application security.

13. Operational security

All the ACS Group information systems that process or store proprietary information must have the appropriate security measures to optimize their appropriate maturity level (monitoring, tracked changes, reviews, etc.). Additionally, networks must be managed, controlled and monitored appropriately to protect against threats and maintain security for systems and applications using the network, including network access controls, thereby protecting all information transferred through these channels and/or environments.

14. Telecoms security

The ACS Group's network architecture must have prevention, detection and response measures to avoid gaps in internal and external domains. “Internal domain” means the local network composed of the ACS Group’s technological equipment accessible exclusively from the internal network. On the other hand, “external domain” means the network accessible from outside the ACS Group network.

Security administration of the networks that cross the ACS Group threshold is of the utmost importance, implementing additional controls for sensitive data that circulate over public communication networks.

Accordingly, the ACS Group shall define the security guidelines to be followed in relation to the transfer of information and the security measures for the use of mobile devices, Internet services and email, together with specific controls that enable secure connection to the ACS Group information systems from outside its facilities.

15. Security in the systems development lifecycle

All systems acquisition, development and maintenance must have the minimum security requirements necessary for the development of software, systems and data in accordance with industry best practices. In addition, test management, tracking of changes and software inventorying should be performed.

Each department of the ACS Group shall take into account the security of information in its systems and data processes, selection procedures, development and implementation of applications, products and services.

16. Security related to service providers

Special attention should be paid to assessing the criticality of all services that may be subcontracted, so that those that are relevant in terms of information security can be identified, either by their nature, the sensitivity of the data to be processed or the dependence on business continuity.

For the providers of such services, selection processes, contractual requirements (such as termination of contract), monitoring of service levels, return of data and the security measures implemented must be treated with a level of care that is at least equivalent to that set out in this Policy.

17. Incident management

All employees of the ACS Group have the obligation and responsibility to identify and notify the Company Security Officer of any incident or offense that may compromise the security of the company's information assets. In addition, the ACS Group shall implement procedures for the correct management of detected incidents.

An incident response management procedure must be created, setting out an incident categorization process, a business impact analysis and escalation by the information security and cybersecurity department for any incident involving information security.

18. Business Continuity

Responding to quality requirements and best practices, the ACS Group shall have a Business Continuity Plan as part of its strategy to ensure continuity in the provision of its essential or critical services and the proper management of business impacts when faced with potential crisis scenarios, providing a framework for the ACS Group to act if necessary. This Continuity Plan must be updated and tested periodically. In addition, a Disaster Recovery Plan aligned with business continuity should be defined and kept up-to-date; this plan shall cover continuity of operation of information and communication technologies.

The ACS Group shall be responsible for the training and competence of all its employees in the area of Business Continuity. Training should be periodically reviewed with the aim of being fully aligned with the existing Plan.

19. Regulatory compliance

The ACS Group shall undertake to provide the necessary resources to comply with all the laws and regulations applicable to its information security activity and to establish responsibility for such compliance with all its members. In this regard, compliance with all applicable laws, standards and regulations shall be ensured.

20. Security Audits and Vulnerability Management

A periodical identification of technical vulnerabilities of the information systems and applications used in the organization must be carried out, evaluating their exposure, and adopting the appropriate measures to mitigate the associated risk.

Once the vulnerabilities have been identified, the company should apply the mitigation measures as soon as possible. The identification, management and correction of vulnerabilities should be done according to a risk-based approach, considering the criticality and exposure of the assets.

21. Exception Management

Any exceptions to this Information Security Policy shall be registered and communicated to the Information Security Officer of the relevant ACS Group company. Such exceptions shall be studied to assess the risk they could create for the Group and, based on the categorization of these risks, these shall be borne by the person requesting the exception and by business managers.

22. Disciplinary sanctions

Any violation of this Information Security Policy may result in appropriate disciplinary action in accordance with the ACS Group's internal process. It is the responsibility of all employees of the ACS Group to notify the Information Security Officer of the company concerned of any event or situation that may result in a breach of any of the guidelines set out in this Policy.

23. Policy review

Approval of this Policy means that Management shall support its implementation in order to achieve all the objectives set out and to meet all its requirements.

This Information Security Policy shall be reviewed and approved annually by the Management Board. However, if relevant changes take place in the company or significant changes are identified in the threat and risk environment, whether operational, legal, regulatory or contractual, it shall be reviewed whenever deemed necessary, so as to ensure that the Policy is always adapted to the actual circumstances of the ACS Group.

24. Annexes

24.1. Annex: Classification levels

Level	Level detail	Examples
Public use	Information that can be known by any type of person and its fraudulent use does not pose any risk to the interests of the ACS Group.	Examples of this type of information are product catalogs and information available on the website.
Limited distribution	Information used by the ACS Group divisions and whose fraudulent use poses an insignificant risk to the Group's interests.	Examples of this type of information are emails and working documents in the Group's divisions.
Confidential information	Information that can only be known to a small number of people and for which fraudulent use can have a significant impact on the interests of the ACS Group.	Examples of this type of information are the Group's audit and strategy reports.
Undisclosed information	Information that should only be known to its owner and whose disclosure could seriously harm the interests of the Group.	Examples are communications between senior managers or shareholders involving decisions relevant to business operations.
Secret information	Information whose unauthorized disclosure may cause exceptionally serious harm to the Group's vital interests.	Examples include employee access passwords, client credentials or encryption keys for accessing systems.