1. Purpose

The purpose of this document is to develop the information security policy and define the basic rules for the acceptable use of information and other assets associated with its processing.

2. Scope

This document applies to the following assets:

- Protected information, i.e. information that allows natural and/or legal persons to be identified, and information relating to the configuration of information systems and communications networks.
- Parties involved in the processing of the aforementioned information (software, hardware, communications networks, information media, auxiliary equipment and facilities).

The processing of information must be carried out in accordance with all security measures that guarantee its:

- Confidentiality: the property of preventing the disclosure of information to unauthorised persons or processes. Confidentiality is access to information only by persons or processes that have the proper authorisation.
- Integrity: this is the property that seeks to keep data free from unauthorised modifications. Integrity is maintaining the information exactly as it was generated, without being manipulated or altered by unauthorised persons or processes.
- Availability: this is the property of being available to those who need to access it, whether they are persons, processes or applications. Availability is access to information and systems by authorised persons or processes when they need it.

3. Specific regulations

3.1. Appropriate use of assets

Information and other associated assets must only be used for the purposes for which they have been made available to users.

The following is expressly prohibited:

- The use of assets provided by Grupo Azpiaran for activities unrelated to their purpose.
- Connecting personal computer equipment that is not approved to the Grupo Azpiaran network.
- Introducing obscene, threatening, immoral or offensive content into Grupo Azpiaran's information systems or corporate network.
- Voluntarily introducing any type of malware (viruses, worms, Trojans, spyware, ransomware, etc.), logical device, physical device or any other type of command sequence that causes or is likely to cause any type of alteration or damage to computer resources into the Grupo Azpiaran corporate network.

- Obtaining rights or access other than those assigned to you by Grupo Azpiaran.
- Accessing restricted areas of Grupo Azpiaran without authorisation.
- Decipher passwords, encryption systems or algorithms, or any other security element involved in Grupo Azpiaran's telematic processes.
- Distorting or falsifying the logs of Grupo Azpiaran's information systems.
- Possess, develop or execute programmes that could interfere with the work of other users, damage or alter Grupo Azpiaran's computer resources
- Destroy, alter, disable or in any other way damage data, programmes or electronic documents containing protected information.
- Storing protected information on the local disk drives of users' PCs, except temporarily for the programming of the development project on which the person is working.

3.2. Confidentiality

Users who have access to Grupo Azpiaran information must consider that such information is, by default, protected. Only information accessed through the public information dissemination channels provided for this purpose by Grupo Azpiaran may be considered unprotected information.

The disclosure, modification, destruction or misuse of information, regardless of the medium in which it is stored, shall be avoided.

The utmost confidentiality shall be maintained indefinitely and no protected information shall be disclosed outside the organisation.

The number of paper reports containing protected information shall be minimised and they shall be kept in a safe place out of the reach of unauthorised third parties (e.g. under lock and key).

In the event that, for reasons directly related to the job, the user comes into possession of protected information contained in any type of medium, they must understand that such possession is strictly temporary, with an obligation of secrecy and without conferring any right of possession, ownership or copying of such information. Likewise, the user must return the aforementioned media immediately after completing the tasks that gave rise to their temporary use and, in any case, upon termination of their relationship with Grupo Azpiaran.

All these obligations shall remain in force after the end of their relationship with Grupo Azpiaran.

Failure to comply with these obligations may constitute a crime of disclosure of secrets.

In addition to the above considerations, in order to guarantee the security of personal data, users must observe the following rules of conduct:

- Files may only be created when necessary for the performance of their work. These temporary files shall never be stored on local disk drives of the user's PC workstations and must be destroyed when they are no longer useful for the purpose for which they were created. Only the programming of the development project on which the person is working may be stored temporarily.
- No personal data shall be stored on the local disk drives of users' PCs.

- The removal of media and documents from the premises where such information is located may only be authorised by the security officer (Systems Manager) in compliance with the security measures contained in this document.
- Media and documents must allow the type of information they contain to be identified, be inventoried and stored in a location with restricted access to authorised persons.
- The transmission of protected information via telecommunications networks (e.g. email) shall not be carried out in clear text. Protected information shall be shared with third parties via SharePoint, encrypting such data or using any other mechanism that ensures that the information is not intelligible or manipulated by third parties.

3.3. Disciplinary procedure

Users who fail to comply with these regulations will be subject to disciplinary proceedings and, where appropriate, sanctions.

Grupo Azpiaran may implement controls to verify compliance with these regulations, without prejudice to compliance with current legislation on the protection of personal data and the right to privacy.

3.4. Return of assets

Users must return all information and associated assets for processing in their possession at the end of their relationship with Grupo Azpiaran.

Access to information and processing assets by all users must be cancelled at the end of their relationship with Grupo Azpiaran or must be adapted to any changes in their duties.

3.5. Physical security

Access to documentation shall be limited exclusively to authorised persons.

The archiving of media or documents shall be carried out in accordance with the criteria set out in the relevant legislation and in accordance with the requirements of the client organisations. These criteria must ensure the proper preservation of documents and the location and consultation of information.

Storage devices for documents containing personal data must have mechanisms in place to prevent them from being opened. When the physical characteristics of these devices do not allow this measure to be taken, measures shall be taken to prevent access by unauthorised persons.

While the media or documents are not stored in the storage devices established in the previous section, because they are in the process of review or processing, either prior to or after their archiving, the person in charge of them must safeguard them and prevent unauthorised persons from accessing them at all times.

The cabinets, filing cabinets or other items in which the media or documents are stored must be located in areas where access is protected by access doors equipped with key-operated opening

systems or other equivalent devices. These areas must remain closed when access to the media or documents is not required.

The creation of copies or reproduction of documents containing specially protected personal data (e.g. health) may only be carried out under the control of persons authorised by the systems manager.

Discarded copies or reproductions must be destroyed in such a way as to prevent access to the information they contain or its subsequent recovery.

Whenever the documentation contained in a file is physically transferred, measures must be taken to prevent access to or manipulation of the information being transferred.

3.6. Documents, media and portable devices

Media, portable devices and documents containing protected information must allow their content to be identified, be inventoried and only be accessible to persons authorised by the security manager.

The removal of media and documents, including those included in and/or attached to an email, from premises under the control of Grupo Azpiaran must be carried out via the corporate SharePoint, authorising individual, non-shared emails. Once the need to share has ended, access will be revoked.

When transferring documentation, measures must be taken to prevent theft, loss or unauthorised access to the information during transport.

Whenever any document or medium containing protected information is to be discarded, it must be destroyed or deleted, taking measures to prevent access to the information contained therein or its subsequent recovery.

Media containing protected information must be identified using comprehensible and meaningful labelling systems that allow users with authorised access to such media and documents to identify their content, while making identification difficult for other persons.

Likewise, portable media and devices must be encrypted, especially when they are outside the Organisation's premises.

3.7. Malware protection

Information systems will be kept up to date with the latest security updates available.

Anti-malware software will be available on Apple, Windows and Android microcomputers.

Anti-malware software must always be enabled and updated.

3.8. Information exchange

No user shall conceal or manipulate their identity under any circumstances.

The distribution of information, whether in electronic or physical format, shall be carried out using the resources specified in the service provision contract for that purpose and for the sole purpose of facilitating the functions associated with that contract.

In relation to the exchange of information, the following activities shall be considered unauthorised:

- Transmission or reception of material protected by copyright in violation of the Intellectual Property Law.
- Transmission or reception of any kind of pornographic material, material of an explicitly sexual nature, racially discriminatory statements, and any other kind of statement or message that can be classified as offensive or illegal.
- Transfer of protected information to unauthorised third parties.
- Transmission or reception of applications unrelated to the business.
- Participation in Internet activities, such as newsgroups, games or others that are not directly related to the provision of the service.

All activities that may damage the image and reputation of Grupo Azpiaran are prohibited on the Internet and elsewhere.

3.9. Use of email

This resource shall be used for professional purposes. Any other use is prohibited.

The interception and/or unauthorised use of other users' messages or email addresses is expressly prohibited.

Users must reject any email messages from unreliable sources, as they may contain viruses or malicious code, spam, etc.

Users must avoid unnecessary disclosure of their email address, mainly by not participating in chain messages, however altruistic their purpose may seem.

3.10. Internet connectivity

This resource shall be used for professional purposes. Any other use is prohibited.

Under no circumstances should users access Internet addresses, games, sexual content, or content that is offensive or violates human dignity or fundamental rights.

3.11. Logical security

Users shall only have access to those resources they need to perform their duties.

Mechanisms shall be established to prevent users from accessing resources with rights other than those authorised.

The systems manager shall be responsible for ensuring that there is an up-to-date list of users and profiles, and the authorised access for each of them.

Only persons authorised (administrators) by the systems manager may grant, alter or revoke authorised access to resources, in accordance with the criteria established by Grupo Azpiaran and the client organisation.

In the event that there are users external to the Organisation, they must be subject to the same security conditions and obligations as internal users.

A mechanism must be established to allow the unequivocal and personalised identification of any user attempting to access the information systems and to verify that they are authorised.

The procedure for assigning, distributing and storing passwords shall guarantee their confidentiality and integrity.

After intervention by a user administrator, the information systems shall automatically force a password change.

The information systems shall automatically force a password change at least once every 90 days, provided that the system allows it and there is no possibility of activating MFA.

Current passwords shall be stored in an unintelligible form.

Passwords must be at least 8 characters long, alternating between numeric, alphanumeric (upper and lower case) and special characters.

Temporary authorised accesses shall be configured for a short period of time and shall be automatically deactivated once this period has expired.

Information systems shall limit the possibility of repeated attempts at unauthorised access to a maximum of 5 attempts.

3.12. User responsibilities

3.12.1. Use of passwords

Under no circumstances should the user disclose their username and/or password to another user or keep it in writing in full view or within reach of third parties.

If the information system does not automatically request it, the user must change the provisional password assigned the first time they log in to the system or when an administrator intervenes.

If the system does not automatically request it, the user must change their password at least once every 90 days, provided that the system allows it and there is no possibility of activating MFA.

The minimum password length must be 8 characters.

Passwords shall consist of combinations of numeric, alphanumeric (upper and lower case) and special characters. It is advisable to use the following rules when selecting passwords:

- Do not use words that refer to recognisable concepts, objects or ideas (e.g. significant dates, days of the week, months of the year, user names, people's names, telephone numbers, etc.).
- The password should be virtually impossible to guess, but at the same time it should be easy for the user to remember (e.g. use the acronym of a phrase or expression, etc.).

If the user suspects that their username and password are being used by someone else, they must immediately change their password and report the incident to ITteam@azpiaran.com.

3.12.2. Equipment

The user must ensure that their PC complies with the following standards:

- When inactive, it automatically locks after a maximum of 10 minutes.
- It does not have:
  - Tools that could violate security measures.

- o Illegal copies of programmes.
- o Non-approved programmes.
- Have up-to-date and activated anti-malware software on Apple, Windows and Android devices.
- Keeps up to date with the latest security updates available.

3.12.3. Workstation

Users must comply with at least the following clean desk rules in order to protect paper documents, computer media and portable storage devices and reduce the risks of unauthorised access, loss and damage to information, both during and outside normal working hours:

- Keep paper documents and computer media under lock and key when not in use, especially outside working hours.
- Lock the session or shut down the user's PC when leaving it unattended.
- Protect both information reception and transmission points (postal mail, scanners and fax machines) and duplication equipment (photocopiers, fax machines and scanners).
- Remove any protected information once printed without undue delay.
- Destroy protected information once it is no longer needed.

3.13. Telework

Teleworking, considered as access to the corporate network from outside the company, shall be regulated by the following rules:

- The use of infrastructure (software, hardware and communications networks) not controlled by Grupo Azpiaran will not be permitted.
- Criteria for authorising teleworking will be established based on the needs of the job.
- The necessary measures will be established for secure connection to the corporate network.
- Security monitoring and auditing systems will be established for the connections established.
- The revocation of access rights and return of infrastructure will be controlled after the period of need has ended.

3.14. Software

Only persons authorised (administrators) by the person responsible for administration may install software.

Users must only use the software versions provided and follow the rules for their use.

The following is strictly prohibited:

- Installing illegal copies of any programme, including standardised programmes.
- Using software that has not been authorised by the administrator.
- Uninstalling any of the programmes installed by Grupo Azpiaran.

3.15. Incidents

An incident is understood to be any unexpected event or series of events relating to information security that has a significant probability of compromising the operations of Grupo Azpiaran and violates these regulations.

When the user detects a possible vulnerability, event or incident, they must immediately notify ITteam@azpiaran.com.

3.16. Regulatory compliance

Compliance with legal restrictions on the use of material protected by intellectual property regulations shall be ensured.

Users may only use material authorised by Grupo Azpiaran for the performance of their duties.

The use of computer programs without the corresponding licence is strictly prohibited.

Likewise, the use, reproduction, transfer, transformation or public communication of any type of work or invention protected by intellectual property rights is prohibited without the proper written authorisation of the owner or rights manager.

Grupo Azpiaran will only authorise the use of material produced by itself, or material authorised or supplied to it by its owner or rights manager, in accordance with the agreed terms and conditions and the provisions of current regulations.

Compliance with current regulations on the protection of personal data in the processing of data of identified and identifiable individuals will be guaranteed.