Information Security Policy for Suppliers

GHSA-POL-06

Ed. 1 01/07/2026

hispasat.com

HispaSat | A part of INDRA GROUP

1. Objective

The main objective of the Information Security Policy for Suppliers (hereinafter the Policy) is to mitigate the potential risks associated with access to information, information systems or resources of the HispaSat Group (hereinafter the Group or HispaSat) by information service providers, regardless of the type of service provided or the nature of their relationship with Hispasat (legal, contractual or any other non-employment relationship), in order to protect the confidentiality, integrity and availability of HispaSat's information and that of its customers. This Policy was approved by the Board of Directors on July 21, 2026, following a favorable report from the Audit Committee. Any amendment shall follow this same procedure.

HispaSat reserves the right to amend this document where necessary. Any changes made will be communicated to all information service providers to whom it applies, using the means deemed appropriate by HispaSat. It is the responsibility of each information service provider to ensure that its staff have read and are familiar with HispaSat's most recent security policies, and to obtain their commitment to comply with and respect these rules.

In the event of a breach of any of these obligations, HispaSat reserves the right to take, in accordance with current legislation, such disciplinary measures as it deems appropriate, which may include the termination of any contracts it has in force with the company in question.

2. General security principles

Information service providers shall provide HispaSat, whenever required, with a list of the individuals, their profiles, roles and responsibilities associated with the service provided, and shall report any changes (new appointments, resignations, replacements or changes in roles or responsibilities) that occur in relation to this list.

Information service providers must ensure that all their staff have the appropriate training and qualifications to carry out the contracted activity, both in terms of the specific subject areas relevant to the service provided and in the field of information security.

Information service providers must ensure, as a minimum, that all staff associated with the service, whether their own employees or subcontractors, are aware of and undertake to comply with the provisions of this Policy. HispaSat may request evidence of the information process at any time. Information service providers must allow HispaSat to carry out the necessary security audits to ensure that the service is provided in accordance with the guidelines set out in this Policy; they must cooperate with the audit team and provide all evidence and records requested.

The scope and depth of each audit shall be expressly determined by HispaSat on a case-by-case basis. Audits shall be carried out in accordance with the schedule agreed in each case with the service provider. HispaSat reserves the right to carry out additional ad hoc audits, if necessary.

2.1. Confidentiality of information

All information, documentation, programmes and/or applications, methods, organization, business strategies and activities relating to HispaSat or its business, to which information service providers have access for the purpose of providing the contracted service, shall be considered confidential information. In accordance with this, access to, exchange of and processing of such information shall always be carried out in accordance with the intended purposes set out in the service provision contract. The information service provider shall, at all times, maintain the requisite duty of confidentiality throughout the duration of the service and after the relationship with HispaSat has ended.

All resources and information to which the service provider may have had access, or which it has been necessary to create, modify or copy for the proper performance of the service, shall be returned upon completion of the service. HispaSat may request the secure erasure of any devices from which access to HispaSat's information has been gained.

2.2. Intellectual Property

Compliance with legal restrictions on the use of material protected by intellectual property legislation shall be ensured. Information service providers may only use material authorized by HispaSat for the performance of their duties. The use of computer software without the relevant license on HispaSat's information systems is strictly prohibited.

Likewise, the use, reproduction, transfer, adaptation or public communication of any type of work or invention protected by intellectual property rights is prohibited without the necessary written authorization. HispaSat will only authorize the use of material produced by itself, or material authorized or supplied to it by its owner, in accordance with the agreed terms and conditions and the provisions of current legislation.

2.3. Protection of personal data

Information service providers carrying out activities for HispaSat who, in the course of their work, may have access to personal data as defined in the specific legislation in force on the matter, must ensure that they comply with current legislation regarding the processing of such data and that they have the required Data Processor Agreements in place.

To safeguard privacy rights, HispaSat is responsible for operating, maintaining and protecting the networks used for its electronic communications. Achieving these objectives involves intercepting and disclosing such communications through automated monitoring systems, log recording and other management tools. By using HispaSat's systems and services, the information service provider using them consents to and permits the monitoring of their profile and that of the professionals involved in the development of the contracted project, with the aim of protecting communications, as well as providing all information stored on HispaSat's resources, where required by a court order or other authority.

In the case of services relating to *cloud* hosting, the location of such infrastructure must be within member states of the European Union. Otherwise, authorization must be sought from HispaSat.

Where, due to the nature of the service to be provided, international data transfers are carried out outside the European Union, such transfers must be expressly authorized by HispaSat and properly documented in accordance with current legislation.

2.4. Exchange of information

Any exchange of information between HispaSat and information service providers shall be deemed to have taken place within the framework established by the relevant service provision contract; consequently, such information may not be used outside that framework or for any other purposes.

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.

HispaSat reserves the right, depending on the identified risk, to implement control, logging and audit measures in relation to these dissemination resources. With regard to the exchange of information within the framework of the service provision contract, the following activities shall be considered unauthorized:

- The transmission or receipt of copyright-protected material in breach of the Intellectual Property Act.
- The 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 may be classified as offensive or illegal.
- The transmission or receipt of sensitive information, unless the electronic communication is encrypted and the transmission is authorized in writing.
- Transfer of protected information to unauthorized third parties.
- Sending or receiving applications not related to business.

- Participation in internet activities, such as newsgroups, games or other activities not directly related to the provision of the service.
- All activities that may damage HispaSat's image and reputation are prohibited on the internet and elsewhere.

2.5. Appropriate use of corporate resources

HispaSat's corporate resources to which information service providers have access shall be used exclusively to fulfil the obligations and purposes of service provision. Under no circumstances may they be used for activities unrelated to the purpose of the service or for carrying out activities that could be considered unlawful, such as infringements of third-party intellectual property rights, breaches of data protection regulations, etc.

Information service providers undertake to use the HispaSat corporate resources to which they have access in accordance with HispaSat's security policies and relevant guidelines.

In order to ensure the proper use of the aforementioned resources, HispaSat may implement such control and audit mechanisms as it deems appropriate, either on a regular basis or whenever deemed necessary for specific security or service-related reasons.

Should it be found that a service provider, or its staff, is misusing HispaSat's resources or information, the provider will be notified of this so that it may take the appropriate action. HispaSat reserves the right to take any legal action available to it to protect its rights.

Any file uploaded to the HispaSat network or to any equipment connected to it via automated media, the Internet, email or any other means must comply with the requirements set out in these regulations and, in particular, those relating to intellectual property, the protection of personal data, and the control of viruses and malicious software.

2.6. User responsibility

Information service providers must ensure that all staff carrying out duties for HispaSat, and who may have access to HispaSat's information, information systems or resources, adhere to the following basic principles in the course of their work:

- Every person with access to HispaSat information is responsible for the activity carried out using their user ID and for everything arising from it. It is therefore essential that each person maintains control over the authentication systems associated with their user ID, ensuring that the associated password is known only to the user themselves and must not be disclosed to other staff under any circumstances.
- Users must not use another user's identifier, even if they have the owner's authorization.
- HispaSat does not authorize the use of passwords agreed upon for use by a group of people as a means of facilitating access to files, applications, databases, computers, networks or other resources.
- Users are aware of and comply with the existing requirements and procedures relating to the information they handle.
- Any user with access to HispaSat information must choose strong passwords (at least 12 characters long, containing upper-case and lower-case letters, digits and special characters, and not containing any easily guessable information such as users' first names or surnames, etc.).

  Under no circumstances shall users store their credentials in a readable format on local files on the devices they use. Nor shall they be written down on paper or kept in places where they can be easily accessed. If there are reasons to believe that a password has been compromised, this must be reported to the Infrastructure & Software Administration department and/or Local IT immediately.
- Any user with access to HispaSat information must change their default and temporary passwords upon their first login, and at least once every 90 days, or whenever there is any indication that other users may be aware of them.
- Anyone with access to HispaSat information must ensure that equipment is secured when left unattended.

- Anyone with access to HispaSat information must adhere to the 'clean desk' policy, in order to protect paper documents, computer media and portable storage devices, and to reduce the risks of unauthorized access, loss and damage to information, both during and outside normal working hours. In this regard, the following practices must be followed: storing information under lock and key, locking down unattended equipment, protecting information reception and transmission points, secure destruction, etc.
- HispaSat information required for the performance of the contracted activities must be stored in locations authorized by HispaSat. Under no circumstances must it be stored locally on computer equipment made available to the supplier's staff. HispaSat does not authorize the storage or processing of its corporate information on equipment for personal use.
- Persons handling information containing personal data that is not stored on a storage device must safeguard it and ensure, at all times, that it cannot be accessed by unauthorized persons. Furthermore, they must comply with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and in Organic Law 3/2018 of 5 December on the Protection of Personal Data and the Guarantee of Digital Rights (LOPDPGDD).
- Persons with access to HispaSat's information systems must never, without written authorization, carry out tests to detect and/or exploit an alleged security weakness or incident.
- It is not permitted to circumvent user authentication or the security of any system, to disclose personal access credentials, to allow the account assigned to oneself to be used by other users—even if they are from the same company or department—or to impersonate another user by accessing or making use of IT resources.
- No person with access to HispaSat's information systems shall, without express written authorization, attempt by any means to breach the security system or authorizations. Users are expressly prohibited from capturing network traffic, unless they are carrying out audit tasks authorized in writing.
- Any conduct contrary to HispaSat's Code of Ethics and Conduct 303-codigo-etico-y-de-conducta-grupo-hispasat_2026-1.pdf is expressly prohibited.

2.7. Security requirements for devices

All devices with access to HispaSat information, regardless of ownership, must comply with the security policies established by HispaSat; in particular, the following considerations must be taken into account:

- Access to systems must always be authenticated, at a minimum, by using a personal identifier and an associated password.
- All software installed on or contained within the device must be licensed, within the product's life cycle and in a state consistent with the license terms.
- Devices must be kept up to date with the latest available security patches for the installed software and operating system.
- Devices must have an anti-malware protection system installed, active and updated to the latest available version, covering both the engine and the signature file.
- The screen lock must be enabled so that it activates after 15 minutes of inactivity. Unlocking must require the use of passwords, unlock patterns or equivalent mechanisms, ensuring that the device cannot be used by an unauthorized user.
- Devices must not contain any tools or files that contravene HispaSat's Security Policy or that may interfere with corporate software. This includes tools that attempt to uncover information other than that of the user themselves or to gain unauthorized access, such as sniffers, network scanning tools, password-cracking tools, etc.

2.8. Reporting of security incidents

Information service providers undertake to report to HispaSat, as soon as possible and in any event within 24 hours, any incident, vulnerability or threat (observed or suspected) that they detect in HispaSat's information systems or that may have affected information belonging to HispaSat or its customers. The report must be made to the relevant department at HispaSat responsible for the service and to the DPO, by sending an email to protecciondedatos@hispasat.com.

Once the provider has resolved the incident that may have compromised HispaSat's systems or assets, the provider must submit a report on the incident, including the causes of the incident, as well as the measures taken to resolve it and prevent similar events in the future.

Where the information service provider acts as a Data Processor, it must follow these guidelines in addition to any provisions set out in the contract governing access to data on behalf of third parties, which has been signed between HispaSat and that provider.

3. Specific security principles

3.1. Physical security

All information service providers whose services are provided from their own premises must take into account the following aspects:

- Buildings or premises must be physically robust (for example: there should be no gaps in the perimeter or areas where breaches could easily occur); the external walls of the premises should be of solid construction.
- All external doors should be adequately protected against unauthorized access through control mechanisms, for example, bars, alarms, locks, turnstiles, CCTV cameras, etc.
- Where possible, it is recommended that physical barriers be put in place which require employees to provide proof of identity via some method of identification and authentication (ID cards, electronic cards, biometric identification, etc.) to prevent unauthorized physical access.
- Buildings or premises should be equipped with automatic detection and response systems for adverse environmental conditions (primarily fire). Where an automatic fire-extinguishing system is not available, manual fire-extinguishing measures must be in place, and all company staff must be familiar with these.
- Basic environmental conditions regarding temperature, hygiene, electrical and acoustic insulation, and other similar measures must be established in accordance with the specific requirements of the IT equipment.
- If any copies of information for which HispaSat is responsible are retained, the systems hosting and/or processing such information must be located in a specially protected area, which must include at least the following security measures:
    - An access control system independent of that of the headquarters.
    - A log of all access events must be maintained.
    - Access by external personnel shall be granted only when necessary and authorized, and always under the supervision of authorized personnel.
    - External personnel may not remain in or carry or carry out work in the specially protected areas without supervision.
    - Have some form of protection against power failures.

3.2. Security in development

All information service providers carrying out application development and/or testing work for HispaSat shall be required to comply with the aspects set out below:

- The environments in which such activities are carried out must be isolated from one another and also isolated from production environments.
- All access to information systems that host or process information must be protected by at least one 'firewall', which restricts the ability to connect to them.
- The entire outsourced software development process shall be controlled and supervised • by HispaSat.
- Application specifications must expressly set out the security requirements to be met in each case.
- Mechanisms for identification, authentication, access control, auditing and integrity shall be incorporated throughout the entire life cycle of the design, development, implementation and operation of the applications.
- Applications developed must incorporate input data validations to verify that the data is correct and appropriate and to prevent the introduction of executable code.
- The internal processes carried out by the applications must incorporate all the necessary validations to ensure that no data corruption occurs.
- Where necessary, authentication and integrity control functions must be incorporated into communications between the various application components.
- The output information provided by the applications must be limited, ensuring that only relevant and necessary information is provided.
- Access to the source code of the applications must be restricted to service staff.
- In the test environment, real data shall only be used where it has been appropriately de-identified or where it can be guaranteed that the security measures applied are equivalent to those in the production environment.
- During application testing, checks must be carried out to ensure that there are no uncontrolled information leakage channels, and that only the intended information is provided via the established channels.
- Only those applications that have been expressly approved shall be transferred to the production environment.

3.3. System Security

All information service providers whose services are delivered through the use of their ICT infrastructure must take into account the following aspects:

3.3.1. Access to network resources and document sharing

- HispaSat will grant staff of information service providers access to its network resources only if necessary for the performance of the work entrusted to them and provided that such access is approved, ultimately by the Infrastructure & Software Administration department.
- The exchange of non-documentary information shall be managed via the channels established by the Infrastructure & Software Administration department. These channels may vary depending on the type of project and the type of information to be exchanged with the information service provider.
- Access to HispaSat's information and applications by an information service provider must be managed in accordance with the current procedure for User Registration, Deregistration and Modification, which specifies that those responsible for the assets to which access is to be granted must request such access from the Infrastructure & Software Administration department via the corporate ticketing system, specifying in that request the users, groups and permissions to be granted to the information service provider.

3.3.2. Asset Management

- Information service providers must maintain an up-to-date asset register in which the assets used to provide the service can be identified.
- Information service providers must notify HispaSat of the decommissioning of assets used to provide the service. If such an asset contains other property belonging to HispaSat (hardware, software or other types of assets), it must be handed over to HispaSat prior to decommissioning so that HispaSat can proceed to retrieve the assets it owns.
- Whenever an asset has contained information deemed sensitive, information service providers must carry out the decommissioning of assets by ensuring the secure deletion of such information, either by applying secure deletion functions or by physically destroying the asset, so that the information it has contained cannot be recovered.
- All assets used to provide the service must have a designated person in charge, who must ensure that such assets incorporate the minimum security measures established by HispaSat, which must at least be those specified in these regulations and, in particular:
    - Comply with the provisions set out in the section 'Security requirements for devices.
    - The most significant events relating to their operation must be logged. These activity logs shall be covered by the provider's backup policy. In particular, all events carried out with privileged permissions must be logged.
    - They must ensure that the system's clocks are synchronized with one another and with the official time.
    - They must ensure that system capacity is managed appropriately, preventing potential downtime or malfunctions of such systems due to resource saturation.
    - You must ensure that the software components associated with protection against intrusions and malicious code on the equipment are updated periodically in accordance with the signature and update releases from the software manufacturer. Furthermore, you must ensure that the equipment has been updated with the latest security patches and is configured to be updated periodically, either automatically or manually. This update must be carried out at least once a month.
    - The information service provider shall ensure that any errors and faults recorded in system activity are analyzed, and that the necessary measures are taken to rectify them.
- The information service provider shall establish a backup policy to ensure that any data or information relevant to the service provided is safeguarded on a monthly basis.
- The information service provider must have secure mechanisms in place for the destruction of any media or documentation that may contain HispaSat information. These mechanisms must ensure that it is impossible to recover any files or data previously stored on them. Should a third-party company be used to carry out the destruction, the information service provider must have entered into the appropriate agreements, having first carried out a prior assessment of that company to verify compliance with current data protection regulations and international standards for Information Security and Privacy (e.g. ISO 27001).
- The information service provider shall have certificates confirming the secure destruction of media or information available to HispaSat for handover once such destruction has been completed.

3.3.3. IT Support

- IT support for the staff of information service providers is the responsibility of each provider. HispaSat's Infrastructure & Software Administration department only deals with:
    - Incidents relating to the IT services provided by HispaSat and set out in this Policy.
    - Incidents or service requests raised by the HispaSat employee responsible for the asset.

3.3.4. Business Continuity Management

- Information service providers must have a business continuity plan and an IT disaster recovery plan in place to ensure the provision of the service even in the event of contingencies. This plan must be developed on the basis of a risk assessment (at least once a year) to identify risks that could cause an interruption to operations and to ensure that appropriate controls are put in place to manage and mitigate them.
- Information service providers shall test the business continuity plan and the disaster recovery plan to confirm that they are capable of restoring the service within the agreed timeframes. These tests shall be carried out at least annually or immediately following any significant changes, upgrades or modifications affecting the services.

3.3.5. Network security

- All networks must be properly managed and controlled, ensuring that there is no unauthorized access or connections whose risks are not appropriately managed by the provider, and establishing the necessary security monitoring and audit systems to guarantee the security of the connections.
- The services available on the networks through which information flows must be limited as far as possible.
- Networks that allow access to HispaSat's infrastructure must be appropriately protected, and the following requirements must be met:
    - They must be notified to and authorized by the Infrastructure & Software Administration • department Remote users' access to the HispaSat network shall be subject to compliance with procedures for prior authentication and access validation by the Infrastructure & Software Administration department.
    - These connections shall be established for a limited period and via virtual private networks or dedicated lines.
    - No communications equipment (cards, modems, etc.) that enables alternative, uncontrolled connections will be permitted for these connections.

3.3.6. Change Management

- Information service providers must ensure that all changes to the ICT infrastructure used to provide the service to HispaSat are controlled and authorized, thereby ensuring that no uncontrolled components form part of the ICT infrastructure.
- It must be verified that all new components introduced into the ICT infrastructure used to provide the service function correctly and fulfil the purposes for which they were incorporated.
- All changes carried out must follow a formally established and documented procedure, ensuring that the appropriate steps are taken to implement the change.
- The change management procedure must ensure that changes to critical components are minimized, being limited to those that are strictly essential.
- All changes to critical components must be verified to ensure that no adverse, collateral or unforeseen effects occur on the operation of those components or on their security.
- Technical vulnerabilities in the infrastructure used to provide the service must be analyzed, and HispaSat must be informed of any vulnerabilities associated with critical components, so that these vulnerabilities can be managed jointly.

Trusted and Reliable
Satellite Solutions

Avda. de Bruselas, 35
28108 Alcobendas
Madrid, Spain
T +34 91 710 25 40

hispasat.com

HispaSat | A part of INDRA GROUP