
	POLICY	DATE: 12/06/2025
		Pág.: 1/16
		Rev. 00
	PO-DTI-SC-003 – Third Party Information Security Policy	


THIRD PARTY INFORMATION SECURITY POLICY

<p>Created by:</p> <p>Felipe de Lara Cybersecurity Analyst</p> <p>Pedro Mota Cybersecurity Analyst</p>	<p>Reviewed by:</p> <p>Rafaela Alcobaça IT Governance Analyst</p> <p>Fernanda Kleis IT Governance Specialist</p> <p>Flavia Segura IT Governance Manager</p> <p>Lucas Correia Cybersecurity Manager</p> <p>Camilla Rocha Vanzella Supply Chain Coordinator</p> <p>Jéssica P. V. Ribeiro Lawyer</p>	<p>Approved by:</p> <p>Marcos Faria TI Director</p> <p>Luiz Fernando Borrego Executive Director of IT</p>
--	---	---

	POLICY	DATE: 12/06/2025
		Pag.: 2/16
		Rev. 00
	PO-DTI-SC-003 – Third Party Information Security Policy	

INDEX

1.	OBJECTIVE	3
2.	SCOPE	3
3.	DEFINITIONS AND ABBREVIATIONS.....	3
4.	ROLES AND RESPONSIBILITIES	4
4.1	CHIEF INFORMATION OFFICER (CIO)	4
4.2	CYBERSECURITY.....	4
4.3	IT GOVERNANCE.....	5
4.4	LEGAL CONTRACT MANAGEMENT	5
4.5	PROCUREMENT DEPARTMENT.....	6
4.6	SERVICE PROVIDERS/SUPPLIERS/THIRD PARTIES.....	6
4.7	HUMAN RESOURCES.....	6
5.	REFERENCES.....	7
6.	GENERAL CONSIDERATIONS.....	7
7.	THIRD PARTY INFORMATION SECURITY REQUIREMENTS IN THE COMPANY’S ENVIRONMENT	8
7.1.1	LOGICAL ACCESS AND ACCEPTABLE USE.....	8
7.1.2	INFORMATION SECURITY INCIDENTS REPORT	9
7.1.3	EQUIPMENT SECURITY.....	9
7.1.4	CONDUCT VIOLATIONS.....	10
8.	SECURITY CONTROLS IN THE THIRD PARTY’S ENVIRONMENT	10
8.13	TRAINING AND AWARENESS.....	15
9	RECORD CONTROL.....	16
10	REVISION CONTROL.....	16
11	ANNEXES	16

	POLICY	DATE: 12/06/2025
		Pag.: 3/16
		Rev. 00
	PO-DTI-SC-003 – Third Party Information Security Policy	

1. Objective

Information is one of the most critical business assets for the GOL Group, and maintaining its confidentiality, integrity, and availability is essential for the Company. The **Third-Party Information Security Policy** aims to establish clear and robust guidelines for protecting the Company's information assets, ensuring the confidentiality, integrity, and availability of data under the responsibility of Third Parties. This policy serves as the foundation for defining security standards, procedures, and controls, aligned with industry best practices and applicable legislation, to mitigate risks, prevent incidents, and ensure compliance with contractual and regulatory requirements. Additionally, it promotes a culture of information security among all stakeholders, emphasizing the importance of protecting assets as an integral part of operations and the relationship between the Parties.

2. Scope

All companies and legal entities that enter into formal contracts with the Company are required to comply with the Information Security requirements outlined herein. Adherence to these guidelines is essential for maintaining effective partnerships and achieving adequate levels of information protection.

3. Definitions and Abbreviations


Company: GOL LINHAS AÉREAS INTELIGENTES S.A and all its direct and indirect subsidiaries, including, but not limited to, GOL LINHAS AÉREAS S.A.

Contract: Any instrument that generates rights and obligations for the Company, including but not limited to contracts, amendments, agreements, letters of intent, termination agreements, notices, and related documents.

Contract Manager: Director, executive manager, manager, or coordinator of the Company, being an employee of the Requisitioning Area responsible for requesting Contracts from the Legal Contract Management Department.

"USER: Do not use unused copies of this document. To do so, make sure that this is the most current version in the electronic document management system before using it."

Uso interno

	POLICY	DATE: 12/06/2025
		Pag.: 4/16
		Rev. 00
	PO-DTI-SC-003 – Third Party Information Security Policy	

Legal Contract Management: Department within the Company's Legal Directorate, composed of the Contract Control Unit and Legal Counsel.

Legal Entity: An entity with rights and obligations, recognized as having legal personality under the Brazilian Civil Code.

Third Party: An individual, entity, organization, and/or its representatives with existing or intended business with GOL. This includes suppliers, contractors, consultants, potential or existing partners.


4. Roles and Responsibilities

4.1 Chief Information Officer (CIO)

- Establish the strategic direction for information security and ensure that security requirements are integrated into the organization's overall strategy;
- Provide resources to implement and maintain adequate security measures related to third-party contracts;
- Ensure that the necessary resources for third-party risk management are available (defined roles and responsibilities, available tools);
- Assume ultimate responsibility for information security and risk management associated with third parties.

4.2 Cybersecurity

- Define information security guidelines for third parties, including security requirements, standards, and procedures to be followed;
- Evaluate third-party security practices, including suppliers and contractors, to ensure they meet the organization's standards;
- Monitor third-party access to the Company's IT systems and resources, applying appropriate access controls;
- Investigate and respond to security incidents involving third parties;

	POLICY	DATE: 12/06/2025
		Pag.: 5/16
		Rev. 00
	PO-DTI-SC-003 – Third Party Information Security Policy	

- Ensure that employees interacting with third parties are adequately trained in information security matters;
- Identify and assess information security risks associated with third parties as necessary;
- Develop strategies to mitigate risks and propose corrective actions when needed;
- Technically analyze and pre-approve Company contracts from an information security perspective, as well as evaluate contractual clauses and conditions when necessary;
- Highlight risks identified in third-party contracts from an information security perspective and recommend necessary adjustments to the Legal Contract Management Department.


4.3 IT Governance

- Verify compliance with information security policies and standards;
- Monitor third-party practices in relation to relevant security regulations and standards;
- Report findings and recommendations to the IT Directorate and Cybersecurity team;
- Support the review and publication of this document.

4.4 Legal Contract Management

- Receive and legally analyze the Company's legal demands, including but not limited to Contracts;
- Direct contractual clauses and conditions related to third-party contracts to the Cybersecurity team for technical analysis and approval;
- Highlight legal risks identified in Contracts related to third-party engagements for analysis and approval by the Contract Manager;
- Legally analyze information security incidents involving third parties when

"USER: Do not use unused copies of this document. To do so, make sure that this is the most current version in the electronic document management system before using it."

	POLICY	DATE: 12/06/2025
		Pag.: 6/16
		Rev. 00
	PO-DTI-SC-003 – Third Party Information Security Policy	

requested by internal departments, especially the Cybersecurity team;

- Draft Contracts, including information security clauses, establishing the rights and responsibilities of the parties, whenever the contract scope requires such inclusion;
- Direct existing contractual clauses in partner, supplier, and customer Contracts to the Cybersecurity team for technical evaluation;
- Legally analyze information security matters when requested by internal departments, especially the Cybersecurity team.

4.5 Procurement Department

- Ensure that requirements are clearly communicated to Third Parties before contracting and formalized in contracts or specific annexes;
- When contracting suppliers whose employees will access the Company's internal network and data, the contracting department must ensure that all employees are trained under the Company's Information Security Training and Awareness Program;
- Maintain an open and transparent communication channel with Third Parties to address information security-related issues.


4.6 Service Providers/Suppliers/Third Parties

- It is the responsibility of these parties to observe and follow the guidelines established for compliance with this Third Party Information Security Policy;
- All activities must comply with applicable laws and regulations, as well as the standards set by regulatory bodies regarding Information Security.

4.7 Human Resources

- Conduct background checks and risk assessments when hiring third parties who will have access to confidential information or critical systems;
- Manage documentation and records related to third parties, including

"USER: Do not use unused copies of this document. To do so, make sure that this is the most current version in the electronic document management system before using it."

	POLICY	DATE: 12/06/2025
		Pag.: 7/16
		Rev. 00
	PO-DTI-SC-003 – Third Party Information Security Policy	

agreements and training certifications.

5. References

ISO/IEC 27005:2019 Information Security Management Systems;

GOL Supplier Support Manual (<https://static.voegol.com.br/voegol/2021-07-19/manual-de-suporte-ao-fornecedor-GOL.pdf>);

GOL Third Party Conduct Guidelines (<https://static.voegol.com.br/voegol/2021-07-19/CartilhaDiretrizesdeCondutaTerceirosnaRelacaocomGOL.pdf>);

PO-SUP-MS-001 - Procurement Policy

6. General Considerations

Third parties/service providers/suppliers must comply with all applicable Brazilian legislation and commit to fully adhering to the following pillars, based on information security best practices:


- Information Security Governance;
- Data Protection;
- Risk Management;
- Account and Access Management;
- Asset Management;
- Operational Security;
- Log and Incident Management;
- Vulnerability Management;
- Secure Development;
- Communication Security;
- Physical Security;
- Business Continuity and Crisis Management;
- Training and Awareness.

They also commit to:

- Protecting information against unauthorized access, modification,

“USER: Do not use unused copies of this document. To do so, make sure that this is the most current version in the electronic document management system before using it.”

Uso interno

	POLICY	DATE: 12/06/2025
		Pag.: 8/16
		Rev. 00
	PO-DTI-SC-003 – Third Party Information Security Policy	


destruction, or disclosure, maintaining its confidentiality;

- Ensuring that resources provided are used only for purposes approved by the Company;
- Ensuring that systems and information under their responsibility are adequately protected;
- Ensuring the continuity of critical business information processing;
- Complying with laws and regulations governing intellectual property;
- Complying with applicable laws related to the Company's activities and market;
- Notifying the Company of any information security incidents that affect the Company's information or operations;
- Service Providers/Suppliers must undergo an Information Security assessment process, including a Self-Assessment, during pre-contract, contract, or post-contract phases.

7. Third Party Information Security Requirements in the Company's Environment

7.1.1 Logical Access and Acceptable Use

- Logical access to the Company's internal network must be requested by the manager responsible for the contract through the ITSM ticketing tool. The request will be evaluated and approved based on necessity, following corporate Information Security and IT Governance guidelines;
- For third parties/service providers/suppliers requiring remote access to the Company's environment, the contract manager must provide access through a unique and individual VPN user account, with access limited to necessary work resources and environments;
- The manager responsible for the third party must inform the validity of the service contract when requesting access and request access removal when

	POLICY	DATE: 12/06/2025
		Pag.: 9/16
		Rev. 00
	PO-DTI-SC-003 – Third Party Information Security Policy	

no longer needed;

- Third-party computers must not be connected to the Company's internal network without prior IT approval and must be protected by antivirus/anti-malware software and other properly licensed software;
- Accessing, downloading, or distributing content that violates copyright or intellectual property rights within the Company's network is prohibited. Similarly, accessing or distributing pornographic content or content that violates the Child and Adolescent Statute is prohibited;
- When applicable, the username and password provided to the third party are for exclusive use and must not be disclosed or shared;
- The third party must keep their access credentials secure and is responsible for any misuse;
- It is the responsibility of the third-party company to notify the Company of any employee departures to ensure their access is promptly revoked; and
- Sharing user accounts and passwords among service providers is prohibited.


7.1.2 Information Security Incidents Report

- Information security incidents and non-conformities known to the third party must be immediately reported to the Company or the contract manager for formal incident notification.
- Once reported, the triage, analysis, treatment, and response process follows the same flow as internal Company incidents.

7.1.3 Equipment Security

- Each user is responsible for protecting physical devices containing Company information under their custody; and
- Each user must be aware that the use of any IT resource in the Company's environment, even if personally owned, is subject to inspection, where local

"USER: Do not use unused copies of this document. To do so, make sure that this is the most current version in the electronic document management system before using it."

	POLICY	DATE: 12/06/2025
		Pag.: 10/16
		Rev. 00
	PO-DTI-SC-003 – Third Party Information Security Policy	

law permits.

7.1.4 Conduct Violations

The following situations, among others, are considered violations of this Policy:

- Any actions or situations that may expose the Company to financial, operational, or reputational loss, directly or indirectly, potentially or actually, compromising its information assets;
- Misuse of corporate data, unauthorized disclosure of information, trade secrets, or other information without the Company's express permission;
- Use of data, information, equipment, software, systems, or other technological resources for illicit purposes, including violations of laws, internal and external regulations, ethics, or requirements from regulatory bodies in the Company's industry; and
- Failure to immediately report any violations of this Policy.

8. Security Controls in the Third Party's Environment


Upon identifying the need, according to the information security and cybersecurity risk assessment criteria set out in the Supplier Risk Management Procedure, the Cybersecurity area will register the supplier in a risk verification tool. The Cybersecurity team will then perform an analysis of the supplier. If the supplier does not achieve the minimum result for the provision of its service, it will be rejected by the Cybersecurity team, until it implements the necessary improvements generated by the platform's recommendation plan.

8.1 Information Security Governance

- The third party must maintain an information security governance structure aligned with industry best practices, such as ISO 27001 and NIST, ensuring compliance with applicable regulations and contractual requirements established by the Company;

"USER: Do not use unused copies of this document. To do so, make sure that this is the most current version in the electronic document management system before using it."

Uso interno

	POLICY	DATE: 12/06/2025
		Pag.: 11/16
		Rev. 00
	PO-DTI-SC-003 – Third Party Information Security Policy	

- A formal information security policy must be in place, addressing data protection guidelines, information classification, access control, and incident management. This policy must be periodically reviewed and disseminated to all employees involved in service provision;
- Third parties must ensure that their employees are continuously trained and aware of information security, participating in educational programs and awareness campaigns to reduce risks related to internal and external threats.


8.2 Data Protection

- The third party must ensure that all personal, sensitive, or corporate data processed complies with the LGPD, GDPR, and other applicable regulations. This includes implementing technical measures such as encryption, pseudonymization, and role-based access control (RBAC);
- Critical data (e.g., passenger information, business strategies) must be stored exclusively in secure environments, with restricted physical and logical access. Data retention beyond the necessary period is strictly prohibited unless formally authorized by the Company;
- The third party is prohibited from sharing, copying, or transferring Company data to unauthorized third parties, even partially. Any exception requires prior written approval from the Company's legal and information security departments.

8.3 Risk Management

- The third party must conduct periodic information security risk assessments of its processes and systems, identifying, analyzing, and treating potential risks that may impact the Company's information security;
- Identified risks that may compromise security or business continuity must be reported to the Company within 48 hours and treated according to

"USER: Do not use unused copies of this document. To do so, make sure that this is the most current version in the electronic document management system before using it."

	POLICY	DATE: 12/06/2025
		Pag.: 12/16
		Rev. 00
	PO-DTI-SC-003 – Third Party Information Security Policy	

established guidelines, with the implementation of appropriate corrective and preventive measures.

8.4 Account and Access Management

The third party must have a formal Access Management process that includes:


- Prohibiting the use of shared or generic accounts, enforcing controls such as mandatory password changes on first login, account lockout after a certain number of failed attempts, and complex password requirements;
- Granting, modifying, and revoking access, especially for privileged accounts;
- Establishing methods for controlling physical and logical access for visitors;
- Implementing VPN and similar controls for remote access by employees during remote work periods;
- The third party must adopt the principle of least privilege and segregation of duties in access management, ensuring that each user has only the permissions strictly necessary for their role;
- Access accounts must be strictly controlled and monitored, ensuring traceability, security, and preventing unauthorized access. Periodic access reviews must be implemented to ensure compliance with the Company's policies.

8.5 Asset Management

- All information assets used must be inventoried, protected, and managed appropriately to prevent unauthorized access, theft, or loss of sensitive data;
- Equipment and systems used for processing Company data must have security controls such as encryption, malware protection, and access control mechanisms.

8.6 Operational Security

"USER: Do not use unused copies of this document. To do so, make sure that this is the most current version in the electronic document management system before using it."

	POLICY	DATE: 12/06/2025
		Pag.: 13/16
		Rev. 00
	PO-DTI-SC-003 – Third Party Information Security Policy	

- Appropriate security controls must be applied to ensure the integrity, availability, and reliability of services provided, preventing failures and cyberattacks;
- Backup and data recovery processes must be implemented and regularly tested to ensure service continuity in case of incidents;
- A backup execution process must be in place, performed periodically on assets storing Company information, to prevent or minimize data loss in the event of incidents.


8.7 Logs and Incident Management

- Ensure the highest level of capability in providing information and adequate management resources for monitoring the services to be provided;
- Inform and provide the Company, upon request, with the necessary management resources for monitoring the contracted services;
- Have dedicated teams and tools for monitoring the capacity and availability of assets, correlating alerts, and generating incident tickets automatically;
- Have a structured Incident Response process, including incident categorization and runbooks for handling and resolving known incidents;
- Keep the Company informed of any limitations that may affect service provision or compliance with applicable laws and regulations;
- Security incidents must be reported within 24 hours via email (csirt@voegol.com.br), following the model stipulated in the contract. The Third Party is responsible for conducting root cause analysis and presenting a lessons learned report within 10 days of resolution. Incidents must be handled according to established procedures, ensuring impact mitigation and the implementation of effective corrective measures.

8.8 Vulnerability Management

- The third party must prevent, detect, and reduce vulnerabilities prone to

“USER: Do not use unused copies of this document. To do so, make sure that this is the most current version in the electronic document management system before using it.”

	POLICY	DATE: 12/06/2025
		Pag.: 14/16
		Rev. 00
	PO-DTI-SC-003 – Third Party Information Security Policy	

materializing as cyber-related incidents, demonstrating best efforts using procedures and controls that include, at a minimum, authentication, encryption, intrusion prevention and detection, data leakage prevention, periodic vulnerability scans and tests, security patch application, server and workstation hardening, malware protection, blocking of unauthorized software, traceability mechanisms, network segmentation, and data backup maintenance;

- Penetration tests (pentests) must be conducted annually on systems/services contracted by the Company. Detailed reports must be shared, including exploitation evidence and remediation recommendations, as well as their mitigation.


8.9 Secure Development

- If the Third Party develops software provided to the Company, it must develop systems considering accepted market security and privacy standards (within the scope of the General Data Protection Law) and OWASP Top 10, integrating Secure Software Development Lifecycle (S-SDLC) practices, including but not limited to:
 - Static and dynamic code reviews.
 - Automated security testing in CI/CD pipelines.
 - Validation of third-party libraries against known vulnerability databases (e.g., NVD).

8.10 Communication Security

- All electronic communications involving Company data must use robust encryption protocols. The use of public networks (unsecured Wi-Fi) for transmitting sensitive data is strictly prohibited;
- Email solutions must be protected by security and secure transfer solutions;
- Inform and provide the Company, upon request, with security measures for

“USER: Do not use unused copies of this document. To do so, make sure that this is the most current version in the electronic document management system before using it.”

	POLICY	DATE: 12/06/2025
		Pag.: 15/16
		Rev. 00
	PO-DTI-SC-003 – Third Party Information Security Policy	

data transmission, storage, and disposal, using secure deletion procedures (media and paper).

8.11 Physical Security

- The third party must ensure that the facilities where services are provided have adequate physical controls, such as access control, surveillance cameras, and asset security.

8.12 Business Continuity and Crisis Management


- Define a business continuity program to ensure that potential incidents do not affect services provided to GOL, including a disaster recovery plan, regularly testing controls to verify preparedness for real cases;
- Copies of the plan must be made available for review by the Company;
- In crisis situations (e.g., ransomware attacks, natural disasters), the **Third Party** must immediately activate a crisis response team, composed of technical, legal, and communication representatives, to coordinate actions with the Company.

8.13 Training and Awareness

- The third party is fully responsible for ensuring that all its employees, directors, shareholders, and intermediaries receive adequate training as part of an annual Information Security and Data Privacy Training and Awareness Program;
- Include in its training and awareness program campaigns such as phishing, social engineering guidance, external lectures, SI and Data Privacy newsletters, etc.;
- Third parties accessing or processing data in the Company's environment must be aware of this Policy and the information security training provided by the Company;

"USER: Do not use unused copies of this document. To do so, make sure that this is the most current version in the electronic document management system before using it."

Uso interno

	POLICY	DATE: 12/06/2025
		Pag.: 16/16
		Rev. 00
	PO-DTI-SC-003 – Third Party Information Security Policy	

- If third-party employees are allocated to work with the Company, either through body shop or resource allocation—i.e., professionals temporarily assigned to work directly with GOL without an employment relationship—they must participate in internal information security and cybersecurity awareness training as indicated by GOL’s Cybersecurity team.

9 Record Control

N/A.

10 Revision Control

Revision	Date	Pages Affected	Description of Modification
00	12/06/2025	All	Initial release in english.

11 Annexes

N/A.