RULES OF PROCEDURE

ATR EIG

CONTENTS

PREAMBLE / SCOPE

In these rules, the ATR EIG will hereafter be referred to as the "**Company**". The purpose of these rules of procedure is to:
- specify the application of the health and safety regulations to the Company;
- determine the general and permanent rules relating to discipline;
- set out the nature and scale of penalties as well as the applicable disciplinary procedure, it being understood that Chapter III devoted to this matter concerns only direct hires and refers the exercise of disciplinary power to the competent hierarchical authority for other types of personnel.

The Rules of Procedure comprise this document and its appendices.

These rules apply to the following persons, regardless of their origin: Company personnel, LEONARDO personnel posted to the EIG, temporary employees, trainees, personnel from external Companies, and any other person authorised to visit ATR sites (hereinafter the "**Personnel**"), in all matters concerning health and safety and the general and permanent rules relating to discipline.

Health and safety provisions apply to all persons present in the facility in any capacity, including:
- the employees of the ATR EIG, regardless of the type of contract binding them to the company,
- the temporary employees,
- the employees of the companies involved,
- the trainees,
- etc.

A copy of these Rules of Procedure is given to each new employee hired in the Company.

CHAPTER 1: HEALTH AND SAFETY

Preventing the risk of accidents and occupational illnesses is a priority for the Company.

In particular, it requires everyone to fully comply with all applicable health and safety requirements, under penalty of disciplinary action.

The provisions aimed at observing the legal and regulatory requirements relating to the health and safety of personnel, the prevention of accidents and, more generally, the prevention of the risks inherent in the activities carried out may be specified by means of memos posted on the signs provided for this purpose and in places where safety instructions must be particularly observed, but also by means of safety instructions or verbal or written recommendations, without this list being exhaustive.

All Staff members must be aware of the health and safety instructions, comply with them and enforce them according to their hierarchical responsibilities within the Company.

In addition, it is the responsibility of each Staff member, in accordance with the instructions given to them by their superiors within the Company pursuant to these rules of procedure and, where applicable, the memos supplementing them, to take care, in accordance with their training, of their own safety and health and that of the other Staff members concerned as a result of their actions or negligence at work.
Violations of all the preceding provisions may possibly result in penalties according to the methods explained in Chapter III hereof.

Article 1. Entry, exit, access to the Company

Article 1.1. Use of the identification badge

Any person working or present within the Company, as well as any Staff member, must always visibly wear the identification badge given to them when they join the Company. This strictly personal badge must be presented whenever requested. Any Staff member leaving the Company permanently must return it before leaving.

Article 1.2. Company access

Access to the Company is authorised to anyone with a valid badge.

Access to or stay in the Company is prohibited, unless authorised by the management of the Company:
- for any Staff member whose employment contract is suspended (example: dismissed, laid off, sick, injured at work, etc.), or exempted from work,
- for any person working on the site (temporary worker, subcontractor) whose employment contract is suspended,
- for any person who does not have an identification badge,
- for any minor individual (with the exception of those holding an internship agreement or an employment contract),
- for anyone with a pet.

Internal travel using rollerblades, skateboards, scooters, unicycles, etc. and/or any other means not authorised by the Management is strictly prohibited.

Article 1.3. Search

Where necessary, in particular in the event of repeated and frequent disappearances of objects and equipment belonging to the Company or for reasons of collective safety linked to the Company's activity (prohibition on bringing hazardous materials, products, etc.), searches may be carried out randomly and on an ad hoc basis, in particular using suitable detection equipment and under conditions that preserve the dignity and privacy of the person. The person concerned will be informed of the right to oppose such inspection. A witness (employee or staff representative) may have to be present during this verification. In the event of refusal by the person concerned, the Management must have recourse to a Police Officer.

Article 1.4. Parking lots - traffic

Staff members are authorised to park their vehicles[1] in the designated parking area, subject to the availability of space, in accordance with the rules laid down in the memos, signboards or other signs.
It is prohibited to enter the site with a trailer or a vehicle occupying a space larger than a parking space.
The use of the parking lot is in no way mandatory for the staff. But it necessarily implies the acceptance and observance of all the provisions defined in the memos. Each user remains responsible for the damage that they or their vehicle may cause to other vehicles as well as to people and property in the vicinity, without the Company being considered, in any capacity whatsoever, as engaging its liability.
Each user undertakes to be insured in accordance with the laws in force for the use of land motor vehicles.
Traffic within the establishment is governed by the rules of the highway code. Each user must follow the signs by using the traffic lanes corresponding to their destination, their category of vehicle and subject to holding the corresponding authorisations.

Article 1.5. Personal items

The Management declines all liability for the loss, theft of or damage to belongings, cash, or objects of any kind left by staff in any place, enclosed or not, within the premises. Identified perpetrators of theft or damage to belongings, cash, or objects are liable to the penalties provided for in Chapter III hereof.

Article 2. General obligations

All staff members are required to:

- Report the following to the hierarchy immediately:
  - Any risk observed or damaged equipment likely to jeopardise safety,
  - any incident that could have had serious consequences,
  - any accident suffered by them during work,
  - any defect in the Company's asset protection systems.

- Report within 24 hours to the Human Resources department any accident of which they have been the victim during their commute.

- Comply with the instructions and requirements, set out in this document, or in any other regulatory document applicable in the Company.

- Use, in accordance with their intended purpose, all collective or individual means of protection made available to them against the risks for which they are intended and strictly observe the specific instructions given for this purpose.

- Use work equipment in accordance with its purpose. The following is considered as work equipment: machines, devices, tools, gear, installations and, in general, any equipment entrusted to the employee for the performance of their work.
  Unless authorised by the Management, it is formally prohibited to use them for other purposes, in particular personal, or to intervene on one's own initiative on any work equipment whose maintenance is entrusted to specialised personnel.
  In the event that the execution work also includes the maintenance or cleaning of work equipment, the employee is required to devote the necessary time to it according to the methods defined by the memo.
  It is reiterated that:
  - any intervention on work equipment, either by a staff member or by a specialist, is subject to the specific instructions given for this purpose: the work requirements must be strictly followed;
  - any stoppage of work equipment or any incident must be immediately reported to the

[1] The definition of the word “vehicle” in the rules of procedure is as follows: any motor or non-motor vehicle allowing movement, and in particular cars, motorcycles, and bicycles.

hierarchy.

- Comply with the rules relating to hazardous substances and preparations: any employee assigned to a workstation exposing them to hazardous substances or preparations must use or handle these substances or preparations in accordance with the instructions given to them by the hierarchy and/or by any work document (ranges, memos, etc.).

- Comply with the basic rules pertaining to order, cleanliness, hygiene, and safety in all the premises used by the Company and especially in the sanitary facilities.

- For access at height and routine handling, use the conventional means provided: stepladders, platforms, handling aids, etc.

- Comply with the rules relating to health and safety determined by the external sites, in particular by Airbus on the Saint-Martin site.

- When workplaces require the wearing of protective equipment or involve access to moving machinery where there is a risk of getting entangled, any loose-fitting garment or accessory which interferes with or prevents the wearing of the required protective equipment is prohibited.

Article 3. Right of alert and withdrawal

- Any Staff member who has reasonable cause to believe that a work situation presents a serious and imminent danger to their life or health may withdraw from their post and must immediately notify their superiors within the Company, or the Human Resources Department, and, if necessary, record in writing all information concerning the danger, which is considered to be serious and imminent, as well as any defect that they observe in the Company's asset protection systems.
  The exercise of the above provision shall not create a new situation of serious and imminent risk for others.

- In the event of serious, imminent danger, any Staff member must, on injunction, stop their activity, move to a safe place and comply with the instructions given by their superiors within the Company, or any person responsible for on site safety.

- In case the working conditions protecting the safety and health of employees appear to be compromised, the Staff may be called upon, at the request of the Company's management, to participate in restoring these conditions in accordance with procedures to be defined from time to time depending on the emergency.

Article 4. Prohibitions

Article 4.1. General prohibitions

No Staff member shall:

- Bring hazardous materials, hazardous , toxic, or narcotic products or alcoholic beverages into the Company premises.
- Use fire and rescue equipment for any use other than that for which it is intended, clutter the locations giving access to this equipment and move this equipment.
- Eat outside the designated premises and use professional equipment for the preparation of meals or drinks.
- Oppose measures stipulated by qualified officers to ensure the safety of the Staff or property.
- Deliberately disrupt, neutralise, or damage safety devices and equipment (collective or individual), modify or move them. Thus, the removal or neutralisation, even partial, of any individual or collective protective device of the equipment by the employees may constitute misconduct. If the slightest problem is observed on a machine, the employee using it must stop its operation using the stop buttons and immediately alert their superiors.
- Wear loose fitting clothing or keep long hair unprotected when working on machines or installations in workshops.

Article 4.2. Prohibition of the use of mobile phones and MP3/MP4 players

As all the buildings on the ATR sites in Toulouse are equipped with emergency evacuation voice systems, and for safety reasons linked to high-risk posts, in particular posts carrying out the following handling operations: moulding/unmoulding, movement/testing of aircraft, driving of machinery, mechanised handling, working at height, handling of hazardous products, and any intervention requiring the employee's full attention, the use of double headphones, MP3, MP4, smart phone, etc. (or, in view of technological developments, any other medium with the same purpose) is prohibited.
Similarly, during interventions in ATEX zones and activities (explosive atmosphere, fuel, etc.), the use of all (non-ATEX) means of this type is prohibited.

Regarding travel with ATR vehicles, and in order to avoid collisions, the use of these devices is also prohibited for drivers when traveling within the company.

Apart from the cases mentioned above, occasional use of mobile phones for personal purposes or for the necessities of everyday life is tolerated.
Any behaviour contrary to these recommendations may result in one of the penalties provided for in these rules of procedure.

Article 4.3. Prohibition of alcohol and illicit substances

It is prohibited to consume or bring into the company premises, alcohol or illicit substances.
The consumption of alcoholic beverages is authorised, in reasonable quantities and in accordance with the legal rate in force, only in the following strictly limited cases:

- as part of a meal eaten at the company restaurant(s),
- in the context of ATR's external and institutional relations, for events taking place at the company restaurant(s).

No employee must enter or stay in the company in a state of intoxication or under the influence of illicit substances.

In view of the obligation of the Site Manager to ensure safety, the Management may impose a blood alcohol test or a saliva test to detect the use of drugs on any person engaged in carrying out work, handling toxic or hazardous products, driving vehicles or using machines in cases where alcohol consumption constitutes a danger for the person concerned and their environment.
These checks may, at the request of the person concerned, be carried out in the presence of a third party of their choice and belonging to the Company.
The person concerned may request a second opinion.
Any positive drug screening test, any overrun of the legal rates in force or refusal to submit to the inspection may result in a penalty.

Receptions organised by any Staff member on the occasion of a wedding, birth, retirement, promotion, etc. may only take place in the Company's restaurant subject to the prior agreement of their supervisors and the Human Resources Department.

Article 4.4: Prohibition on smoking

Smoking is strictly prohibited inside all buildings, in the means of transport provided by the company, on the movement and parking areas for aircraft, and on the exterior areas marked with “No smoking” signs (ATEX zone, etc.).
It is prohibited to throw cigarette butts outside the ashtrays, and to smoke in front of the entrances to the buildings. Smoking shelters are available.
This prohibition applies to all kinds of cigarettes or cigars, including electronic cigarettes.
Regardless of the penal sanctions provided for in this regard, any non-compliance with one of the provisions set out above is misconduct and will therefore be liable to one of the penalties provided for in these rules of procedure.

Article 5. Occupational health

All Staff members must respond to calls from the Occupational Health Department relating to:

- preventive and informational or pre-recruitment medical visits,
- periodic medical visits,
- special medical visits related to the activity by regulation,
- specific medical visits decided by the Occupational Health Department as part of its preventive action,
- work resumption medical visits in the cases provided for by the Labour code (Article R4624-31):
  - medical visits after maternity leave;
  - medical visits after an absence due to an occupational illness;
  - medical visits after an absence of at least thirty days due to an accident at work, non-occupational accident or illness.
- medical visit at the employer's request, irrespective of periodic examinations.

CHAPTER 2: DISCIPLINE

The provisions of this chapter apply to all Staff subject to trade union rights and staff representation.

Article 1. Working hours

In accordance with legal requirements, the working hours are set by the Company's Management and brought to the attention of the Company's Staff by memorandum and posting (on notice boards and/or intranet).
They are likely to vary according to the needs of the service or the arrangements specific to the variable schedule in compliance with the employment contract.

All Staff members must follow the weekly work schedule as well as the badge rules applicable to them before and after meals and in the evening while leaving. Any delay must be justified to their immediate supervisors within the Company.

No Staff member may, during working hours, leave their work place without reasonable cause or leave the Company premises without authorisation.

It is strictly prohibited to clock in and out for another Staff member or to clock in and out irregularly.
Any failure to clock in must be justified and regularised with the supervisor within 24 hours in the time management tool.
The Staff may not refuse to work overtime requested under the legal exemptions.

Failure to comply with these timings may result in penalties.

Article 2. Execution of work

In carrying out the tasks entrusted to them, the Staff must comply with the directives given to them by their supervisors within the Company.

Article 3. Absences

Any absence for illness or for any other medical reason must be reported to the supervisor as soon as possible by any means, and justified within 3 days by sending a medical certificate (in the “CERFA” form) to the payroll management department.
Any absence for any other reason, regardless of its duration, must be the subject of a request approved by the supervisor within the Company and sent to the Human Resources Department (as per the practical arrangements in force)[2] no later than the day before, and must be justified. If, for a case of force majeure, such a request could not be presented, the absence must be justified within 48 hours.

Article 4. Dress code / Wardrobes

In view of the company's activity, and in order to maintain its brand image, correct dress is required of staff present in the offices or who may be in contact with customers in general.
The Company receiving customers is part of the “public space” within the meaning of the provisions of Law No. 2010-1192 of 11 October 2010, it is therefore prohibited for each employee to wear an outfit

[2] For information, depending on the reason for the absence, this may be in particular through the time management tool, or registered letter with acknowledgment of receipt or hand-delivered against receipt to the Human Resources department.

intended to conceal their face.. The same is true for employees likely to carry out their duties outside the Company's premises.

Members of the Company's staff are required to wear work clothes (trousers, T-shirt, jacket, jumper, etc.) and personal protective equipment (shoes, gloves, masks, overalls, etc.) provided to them on the Company's premises.

Work clothes maintained by the company must remain within the company premises, it is prohibited to take them outside the premises.
Employees wearing specific work clothes must not leave work or street clothes and personal tools anywhere other than in the changing rooms or designated area. Thus, in accordance with Article R. 4228-6 of the Labour Code, individual wardrobes are provided with a padlock or a lock, a means of closure for which each employee is responsible. These wardrobes must only be used for the purpose for which they are intended, they must be identified by name and always be kept clean. For health and safety reasons, the employer may have these individual wardrobes opened in the presence of the employee concerned, having ensured that they are informed beforehand. In the event of absence or refusal of the parties concerned, the employer reserves the right to proceed in the presence of two witnesses.

Article 5. Use of Company-owned equipment

The Equipment, i.e. all the professional tools made available to the Staff (e.g. mobile phone, e-mail, software, Mobile Elevating Work Platform, etc.) remains the sole and exclusive property of the Company and must be used by the Staff only as part of their duties within the Company.
Under no circumstances is the Staff granted the right to appropriate, and/or assign, and/or transfer all or part of the Equipment.
Their use, unless authorised by the Management, is reserved for professional purposes. However, the use of professional emails or mobile phones for personal purposes is tolerated on the sole condition that it is done within reasonable limits, that is to say briefly and occasionally.

During their time with the Company, the Staff must ensure that they take all appropriate steps to preserve the security and integrity of the Equipment.

Article 6. General discipline

Every employee must follow the basic rules of professional conduct and manners.

Any brawl, insult, aggressive behaviour, or incivility is prohibited in the Company, all the more so when this behaviour is likely to be penalised.
The same applies to any racist, xenophobic, sexist and/or discriminatory behaviour within the meaning of the provisions of the Labour Code and the Criminal Code.

Any act contrary to professional obligations or likely to disrupt the smooth running of the Company may fall within the scope of Chapter III of these Rules.
By way of example and non-exhaustively, the following are considered as such:

- To instigate, commit or allow to be committed, any illegitimate act likely to disturb the order within the Company or the discipline of the Staff.

- To introduce or facilitate the introduction into the Establishment of goods, publications and documents of any kind intended to be sold or distributed (except for exhibitors from outside the company restaurant with the authorisation of the Works Council).
- To be absent from one's workstation, leaving one's workstation, moving around the establishment without a valid reason and without authorisation from the supervisors.
- To stay for an inordinate amount of time in front of beverage dispensers.
- To remain inactive at your workstation and/or voluntarily limit productivity.
- To remain at the workstation outside of working hours without any valid reason.
- To carry out personal work and, more generally, engage in any occupation other than that resulting from the job held or ordered by the responsible hierarchical authority.
- To remain in the Establishment in the event of an evacuation order given by the Management.

- To provoke verbal or physical altercations with colleagues, make remarks likely to provoke incidents, degrade working conditions and/or the dignity of people
- To enter premises other than those where one's duties are carried out, unless authorised by the supervisor.
- To use the company's franking service for personal purposes.
- To engage in any form of religious or political propaganda.
- To put up inscriptions on buildings, machines, equipment.
- To obstruct in any way the entry and exit of personnel or equipment, in particular by staying around accesses.
- To interfering in any way with the freedom to work.
- To disclose to third parties information of any kind concerning the company's activity, studies and projects, manufacturing processes or to communicate information to anyone (even staff members) who is not authorised to receive it.
- To take photographs or make drawings of buildings, machines, work in progress, and in general of any equipment or document in the company, without prior authorisation from the supervisor.
- To display within the Company, without the authorisation of the Company's management, leaflets, newspapers, printed matter, or documents of any kind whatsoever, outside the spaces reserved for this purpose.
- To tear up, destroy, and cover up posters put up by the Company's management.
- To take away from the Company, without the authorisation of the Company's management, Documents and/or Information, and/or equipment, belonging to the Company, even if they are out of order or of no value.
- To provoke or organise non-professional meetings, demonstrations, subscriptions, or ceremonies (not provided for in collective agreements or regulations) in the Company without authorisation from the Company's management.
- To park vehicles in places not intended for this purpose (aisles between car parks, lawns, etc.) or reserved places (airlines or customers, visitors) on the Company's site.
- To not respect speed limits within the Company premises.

Article 7. Additional provisions

The commercial and international nature of the Company implies frequent contacts with representatives or clients from countries different from our own and, consequently, from communities sometimes diametrically opposed to the one we know.

It is therefore strongly recommended that staff in contact with outsiders take care in their choice of dress so as not to offend the sensibilities of our visitors.
It is also recommended that all Staff members protect, during such visits to the Company, any Document and/or Information and/or equipment, which may be directly and/or indirectly within the reach of such visitors.

Article 8. Provisions on psychological and sexual harassment

Article 8.1. Provisions on psychological harassment

Article L.1152-1
No employee shall be subjected to repeated acts of psychological harassment intended to cause or resulting in damage to their working conditions likely to infringe their rights and dignity, to alter their physical or mental health or to compromise their professional future.

Article L.1152-2
No employee, trainee, or intern may be penalised, dismissed, or subjected to a direct or indirect discriminatory measure, in particular with regard to remuneration, training, reclassification, assignment, qualification, classification, professional promotion, transfer or renewal of contract, for having been subjected to or refused to be subjected to repeated acts of psychological harassment or for having witnessed such acts or having reported them.

Article L.1152-3
Any termination of the employment contract in disregard of the provisions of Articles L. 1152-1 and L.

1152-2, or any provision or act to the contrary, shall be void.

Article L.1152-4
The employer shall take all necessary steps to prevent psychological harassment.
The text of Article 222-33-2 of the Criminal Code is displayed in the workplace.

Article L.1152-5
Any employee who engages in acts of psychological harassment is liable to disciplinary action.

Article L.1152-6
A mediation procedure can be implemented by any person in the Company who considers themselves to be the victim of psychological harassment or by the person in question.
The choice of mediator is subject to an agreement between the parties.
The mediator inquires about the state of relations between the parties. They try to reconcile them and submit proposals to them, which they record in writing in order to put an end to the harassment.
When reconciliation fails, the mediator informs the parties of any penalties incurred and the procedural guarantees provided for the victim.

Article 8.2. Provisions on sexual harassment

Article L.1153-1
No employee should be subject to the following:
“1° Sexual harassment, consisting of repeated comments or behaviour with a sexual connotation which either violate their dignity because of their degrading or humiliating nature, or create an intimidating, hostile or offensive situation for her;”

“2° Conduct amounting to sexual harassment, comprising any form of serious pressure, even if not repeated, exercised with the real or apparent aim of obtaining an act of a sexual nature, whether this is sought for the benefit of the perpetrator or a third party.”

Article L.1153-2
No employee, trainee or intern, recruitment, internship or training candidate in the Company may be penalised, dismissed or be the subject of a direct or indirect discriminatory measure, in particular with regard to remuneration, training, reclassification, assignment, qualification, classification, professional promotion, transfer or renewal of contract, for having been subjected to or having refused to be subjected to acts of sexual harassment as defined in Article L. 1153-1, including, in the case mentioned in 1° of the same article, if the comments or behaviour have not been repeated.

Article L.1153-3
No employee, trainee, or intern may be penalised, dismissed, or subjected to any discriminatory measure for having witnessed or reported sexual harassment.

Article L.1153-4
Any provision or act contrary to the provisions of Articles L. 1153-1 to L. 1153-3 is void.

Article L.1153-5
The employer takes all necessary measures to prevent acts of sexual harassment. The text of Article 222-33 of the Criminal Code shall be displayed in the workplace and on the premises or at the door of the premises where recruitment takes place.

Article L.1153-6
Any employee who has engaged in sexual harassment is liable to disciplinary action.

Article 8.3. Legal actions

Article L.1154-1
When a dispute arises relating to the application of Articles L. 1152-1 to L. 1152-3 and L. 1153-1 to L. 1153-4, the candidate for a job, an internship, or a training period in the Company where the employee presents factual elements suggesting the existence of harassment.
In view of this information, it is up to the defendant to prove that these actions do not constitute such harassment and that its decision is justified by objective factors unrelated to any harassment.
The judge shall form their opinion after ordering, if necessary, all the investigative measures they consider

useful.

Article L.1154-2
The representative trade union organisations in the Company may bring all actions resulting from Articles L. 1152-1 to L. 1152-3 and L. 1153-1 to L. 1153-4 before the courts.
They may exercise these actions in favour of an employee of the Company under the conditions set out in Article L. 1154-1, subject to the written agreement of the person concerned.
The person concerned can always intervene in the proceedings initiated by the union and put an end to them at any time.

Article 8.4. Penal provisions

Article L.1155-1
The fact of interfering or attempting to interfere with the regular performance of the duties of a mediator, as provided for in Article L. 1152-6, is punishable by one year's imprisonment and a fine of €3,750.

Article L.1155-2
Acts of discrimination committed as a result of psychological or sexual harassment as defined in Articles L. 1152-2, L. 1153-2 and L. 1153-3 of this code are punishable by one year's imprisonment and a fine of €3,750.
The court may also order, as an additional penalty, the posting of the judgment at the expense of the convicted person under the conditions set out in Article 131-35 of the Criminal Code and its publication, in full or in extracts, in the newspapers it designates. These expenses may not exceed the maximum amount of the fine incurred.

Article 8.5. Provisions common to psychological harassment, sexual harassment, and violence at work, in application of Articles 3 and 5 of the interprofessional agreement of 26 March 2010.

Principle:
Acts constituting sexual harassment, psychological harassment, and violence at work are not permitted in the Company.

Procedure:
An employee who is the victim of acts constituting psychological harassment, sexual harassment, or violence at work shall inform the employer in writing of the following:

1. a precise description of the events of which the employee considers themselves to be the victim;
2. their dates;
3. the identity of the person or persons allegedly involved in these events;
4. the possible filing of a complaint.

Upon receipt of this letter, the employer initiates an adversarial investigation in order to verify the facts and to take, if necessary, the necessary measures.

During this investigation, the employer ensures that the employee victim is not subjected to any risk of recurrence of the events.

Penalties:
The penalties applicable to perpetrators of psychological harassment, sexual harassment, or violence at work are those provided for in Chapter 3 of these rules of procedure.

Deliberate false accusations must not be tolerated, and may result in the disciplinary measures set out in Chapter 3 hereof.

Article 9. Provisions on gender-based harassment

Article L.1142-2-1
No one shall be subjected to gender-based harassment, defined as any harassment related to a person's gender that has the purpose or effect of violating their dignity or creating an intimidating, hostile, degrading, humiliating, or offensive environment.

Penalties:
The penalties applicable to perpetrators of gender-based harassment are those provided for in Chapter 3 of these rules of procedure.

Deliberate false accusations must not be tolerated, and may result in the disciplinary measures set out in Chapter 3 hereof.

Article 10. Integrity and ethics principles

The ATR GIE is subject to a Code of Business Conduct which prescribes rules and conduct applicable to the operation of the company and to all employees and external personnel (temporary workers, trainees, subcontractors, employees provided).

The Code of Business Conduct defines essential concepts, refers to key documents and procedures, and contains guidance.
It illustrates in particular the different types of behaviour to be prohibited as it is likely to be considered as bribery or influence peddling.
This code is appended to these rules.

Failure to comply with these provisions is likely to result in penalties as provided for in Chapter 3 of these rules.

CHAPTER 3: DISCIPLINARY SANCTIONS

This chapter is directly applicable to Staff members directly bound to the Company by an employment contract. With regard to other Staff members and mainly employees posted by the members, it will be up to each initial employer and holder of the disciplinary power to assess the seriousness of the facts brought to its attention by the Company's management.

Article 1. Nature and scale of penalties

Any act considered to be wrongful may, depending on its severity, be subject to one or the other of the following penalties:

- Minor penalties:
  - written comment,
  - warning.
- Major penalties:
  - disciplinary layoff from 1 day to 15 working days depending on the seriousness of the misconduct (temporary suspension of the employment contract without pay),
  - disciplinary transfer, i.e. change of position for disciplinary purposes subject to compliance with the employment contract,
  - demotion, i.e. assignment to a different and lower-level function, subject to the employment contract,
  - dismissal with notice, severance pay, and holiday pay,
  - dismissal for serious misconduct, without notice or severance pay, but holiday pay,
  - dismissal for gross negligence without notice, nor severance pay but holiday pay.

The order of listing is not binding on the Company’s management and the list above is not exhaustive.

Article 2. Definition of misconduct

Misconduct shall be deemed to be conduct manifested by a positive act or voluntary abstention that does not correspond to the normal performance of the contractual relationship. This may include non-compliance with a provision of the rules of procedure, the labour code, as well as the non-performance or poor performance of one’s duties.

Article 3. Employee rights

No misconduct alone may give rise to disciplinary proceedings after a period of two months from the day on which the employer became aware of it, unless it has given rise to criminal proceedings within the same period.
The initiation of proceedings is in principle constituted by the summons to the preliminary interview or the declaration of a precautionary layoff.

No penalty older than 3 years prior to the initiation of disciplinary proceedings may be invoked in support of a new sanction (Art. L. 1332-5 of the Labour Code).

No penalty can be imposed on the employee without informing them at the same time in writing of the grievances against them.
No penalty, other than a warning or a written observation, may be notified until the person concerned has been called to a preliminary interview.
They may be assisted by a person of their choice from the Company's staff.

Following this interview, the possible penalty will be notified to them in writing, stating the reasons, and may not take place less than two working days nor more than one month after the day set for the interview.
If the employee's conduct has made a precautionary layoff measure essential with immediate effect, the final penalty relating to this action can only be taken by following the procedure set out above.

CHAPTER 4: FILING, PUBLICITY AND ENTRY INTO FORCE

Article 1. Formalities, filing

In accordance with the requirements of Article L. 1321-4 of the Labour Code, these rules have been:

- submitted for opinion to the social and economic committee on 22 April 2021,
- communicated in duplicate to the Labour Inspector governing the Company on 28 April 2021,
- filed in one copy with the Court Registry of the Toulouse industrial tribunal, on 28 April 2021.

Article 2. Modification

Any subsequent modification, addition or withdrawal pertaining to these rules shall be subject to the procedure set out in Article 1 of this chapter, in accordance with the provisions of Art. L. 1321-4 of the Labour Code.

Article 3. Memoranda or other additional documents

These rules of procedure may be supplemented by memos or other additional documents (memo, charter, code, directives, etc.) containing general and permanent requirements that the Management deems necessary.
These documents are either distributed by the Human Resources department to employees, or posted on the boards reserved for this purpose and/or on the intranet and are subject to the same consultations and the same formalities as these rules.

Article 4. Entry into force

These rules of procedure will enter into force on 3 June 2021, and completely replace the provisions of the rules of procedure in force previously.

Article 5. Enforceability

These rules may be invoked against all employees referred to in the preamble hereto, whether they were hired before or after the entry into force thereof.

All employees are required to read these regulations at the time of their hiring. No employee will therefore be able to claim ignorance.

Blagnac, 28 April 2021

Appendices

1. ATR charter for the secure use of ATR information system and technology resources

2. Code of conduct applicable within the ATR GIE in terms of integrity and ethics

ATR CHARTER FOR THE SECURE USE OF THE ATR INFORMATION SYSTEM AND TECHNOLOGY RESOURCES

(INTRANET, INTERNET, EMAIL, TELEPHONY, ETC.)

PREAMBLE

For the attention of users of the ATR information system and technologies:

Your professional activity within the Company implies the provision of access to internal and external IT systems (computers, networks), together with a personal right of access to the functions and data they contain (e.g. email or the Intranet).

We speak of information systems and technologies, hereafter referred to as Is&T resources.

Internal systems and their data are part of the company's assets, necessary for its operation and therefore protected as such. As a recognised and authorised user, you shall ensure their proper use in the same way as you would any other work tool. It is up to you to make rational use thereof, both from a technical and ethical point of view.

On the other hand, certain systems such as the Internet network, made up of a mesh of multiple open networks, are external sets that do not belong to the Company, with uncontrolled and unguaranteed use. In particular, the Internet network does not guarantee the integrity and confidentiality of the data transmitted, as well as the authenticity of the data collected or the anonymity of the users. Although all security measures are taken by the IT departments, connecting to such networks presents risks for your data, your workstation, and the company's IT systems, against which it is necessary to protect yourself.

Since your exchanges on the Internet in a professional capacity are under the company’s name, this activity can engage your individual responsibility but also that of ATR, and its brand image.

Consequently, it is the responsibility of the Company to implement ethical rules for access and use of computer systems (particularly for access to the Internet) and appropriate technical means (anti-virus) to protect our tool from any risk of destruction, intrusion, or alteration. It is your responsibility to comply with these rules and these means.

The purpose of this charter is to set out the recommendations for accessing and using internal and external computer systems from your workstation, and the precautions to be taken. It allows you to integrate good practices in your conduct while using our systems.

It also informs you of your responsibility and of the control put in place by ATR to protect its systems and assets. This control makes it possible to track your use of the tools made available to you.

We request you to read this charter and count on your collaboration in its application and compliance therewith.

CONTENTS

1- PURPOSE & SCOPE

The purpose of this document is to inform users of the rules applicable to the use of IS&T resources (information systems and technologies).

The rules contained in this document apply regardless of whether the user uses IS&T means on or off ATR sites.

The objective of these rules is to guarantee the confidentiality, integrity, and availability of all the operations and all the interests of ATR. In accordance with this objective, ATR's Digitalisation Department is entitled to monitor and control the use of IS&T resources by all users.

2- USE OF IS&T RESOURCES

2.1 GENERAL USE

Users are authorised to use the IS&T resources in the context of their professional tasks, provided that such use complies with the security provisions and ethical standards described in this charter and supplemented by additional internal rules.

This document is communicated to all users.

To enable coordination of immediate action, any risk of a security breach (including but not limited to: phishing emails, virus infection, loss or corruption of data, theft of equipment, fraudulent use of a user account, unauthorised access to data or transmission of offensive content) should be reported immediately to the ATR Digitalisation Department (via the helpdesk).

Users acknowledge that all activities conducted on an ATR email address or via the ATR Network could be interpreted by outsiders as actions of ATR. Therefore, any activity performed by users using IS&T resources may impact ATR.

2.2 PERSONAL USE

The use of IS&T means for personal purposes is expressly prohibited, except in the cases provided for in the following paragraph.

Occasional use of IS&T for personal purposes, e.g. to contact relatives or to carry out everyday tasks, is tolerated as long as it is done without abuse.
Such use of IS&T resources shall:

- comply with the regulations and not be contrary to the interests and rules of procedure of ATR;
- respect the security and integrity of IS&T resources;
- not interfere with or impede the user's job performance or responsibilities.

Any content accessible via, transmitted through, or recorded on the IS&T resources is considered to be professional, unless such content is clearly identified as “Private” or “Personal” (hereinafter referred to as “Private Data”).

All private data should be saved by users in their “Private” or “Personal” folder. A “My Documents” folder, or any other “personal directory”, is not considered private data, unless it is specifically marked “Private”

or “Personal”.

Users are responsible for managing their private data. ATR will not be held liable in the event of loss, destruction, or illegal interception by a third party of private data transmitted or recorded on the IS&T resources.

It is the user's responsibility to remove all private data from IS&T resources before returning a device to ATR for any reason. ATR will not be held liable for direct or indirect damage resulting from the fact that the user has not deleted their private data on the IS&T resources at the end of their assignment/employment contract.

If a user discovers that they have access to another user's personal data, they must immediately contact the helpdesk.

2.3 GENERAL PROHIBITED ACTIVITIES

Users are expressly prohibited from using IS&T resources to carry out, in particular:

- any illegal activity;
- any activity contrary to the interests of ATR;
- any activity aimed at promoting the commercial activities of a third party;
- any activity aimed at promoting the user's external commercial activities.

Users shall not engage in activities that harm or are likely to harm the operations, interests, reputation and relationships of ATR, its customers, suppliers, and partners.

Users shall not damage or affect the interests or privacy of third parties through the IS&T resources.

In addition, the following activities are expressly prohibited for users (non-exhaustive list):

- Authorise people outside the Digitalisation Department to access IS&T resources for maintenance and/or configuration purposes;
- Share their personal passwords and access codes or attempt to obtain the passwords or access codes of other users, including members of the Digitalisation Department;
- Bypass user authentication steps or any other security mechanism for IS&T resources;
- Use and/or install software and/or any application not supplied by ATR or without authorisation from ATR;
- Disable anti-virus programs or any other protection software installed by the Digitalisation Department;

- Record, delete, copy, or duplicate for personal purposes any information, data, or software belonging to ATR without its prior authorisation;
- Commit breach of security or disruption of network communications (breaches of security include, but are not limited to, accessing data for which the user is not the intended recipient, logging into a server or account that the user is not expressly authorised to access);
- Introduce malicious programs and/or applications into the IS&T resources (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.);
- Install or connect to an ATR infrastructure and/or network any unauthorised electronic device (wireless or wired, gateways, bridges, 4G Internet devices) that may affect the operation of the network and generate risks of unauthorised access;
- Modify in any way the configuration of the IS&T resources without the prior authorisation of ATR

provided by the Digitalisation Department.

3- EMAIL

3.1 GENERAL USE

ATR email accounts are reserved for professional use only. All emails sent and/or received on ATR email accounts are deemed to be professional and should, therefore, be subject to ATR's rules regarding the protection and classification of information. The occasional personal use of emails will be tolerated as long as it complies in particular with the provisions of Article 2.2.

3.2 PRIVATE USE

The occasional private use of email to contact family and friends and to carry out daily tasks is tolerated, provided that it does not interfere with normal professional email traffic and that it complies with the provisions of Article 2.2 of this charter and other applicable requirements and limitations as may be set forth in this document.

3.3 GENERAL RESTRICTIONS

The following measures and restrictions will apply to the use of emails:

- In order to detect and avoid threats such as in particular viruses, Trojan horses, worms, identity theft, malicious spam and phishing/vishing messages, the content of all e-mails users will be monitored by ATR's antivirus tools.
  For security reasons, the antiviruses in our systems monitor incoming mail and potentially block a message recognised as containing a virus.
- Notwithstanding these filtering measures, in the event of receipt of a suspicious e-mail, the user must not open the attachments or links it contains, nor send this email to another user. In this case, the user must promptly report any suspicious email received to ATR's Digitalisation Department.
- The user must send any strategic or sensitive information in accordance with the confidentiality rules described in Article 7 of this document.

3.4 PROHIBITED USES

In all cases, users are prohibited (non-exhaustive list):

- To solicit, create, or disseminate unprofessional material, such as chain letters, photos, video or audio files, jokes, unsolicited messages, junk mail or other messages of an advertising nature, inside or outside of ATR;
- To manipulate emails for unauthorised purposes, for example by forging the information of email headers, or by modifying or deleting the footer of outgoing messages;
- To use the ATR mailing lists for non-professional purposes;
- To open, save, or execute an attachment of an email, except if this attachment is deemed reliable;
- To click on hyperlinks that establish a connection to unknown websites;
- To disclose information such as login IDs and passwords, which would allow the recipient to illegally access the IS&T resources;
- Post ATR email addresses on public websites, thereby causing those addresses to be added to spam or mass mailing lists;
- Under no circumstances should users forward work-related emails and attachments to their private storage devices, including but not limited to their private email accounts, private cloud accounts,

or their private storage devices.

3.5 SPECIFIC ACCESS

A user granted access to another user's account for specific purposes in accordance with ATR's policy ("Specific Authorised Access") will need to meet the following requirements:

- The specific authorised access must be the subject of a written agreement from the user whose account is accessed;
- The specific authorised access must be granted for a defined duration.

3.6 EXCEPTIONAL ACCESS

In the event of absence or unexpected departure of a user, it may be impossible for them to provide the written authorisation provided for in Article 3.5. In this case, the IT team, subject to an assessment of the urgency of the need to access the account by the Legal and HR Departments, will authorise a specific person to access the email account of the absent user.
This access will only be authorised if it complies with the local laws in force.

3.7 ACCOUNT CANCELLATION

The choice of transfer or cancellation of a user's email account leaving ATR is given to each user in the exit circuit form. On the date of cancellation of an email account by ATR, the inbox is retained for one month.

4- INTERNET/INTRANET

4.1 GENERAL USE

Access to the Internet/Intranet via IS&T resources, including remotely, is authorised for exclusively professional use.

4.2 PRIVATE USE

Occasional private use of the Internet via IS&T means is permitted for the purpose of contacting family and friends and carrying out daily tasks, provided that it does not affect the normal functioning of the Internet/Intranet and that it complies with the provisions of Article 2 of this document, as well as with the other requirements and limitations in force, as set out here.

4.3 GENERAL RESTRICTIONS

All connections to the Internet/Intranet via IS&T means will be established via standard ATR services (Internet access, remote access).

4.4 PROHIBITED USES

In any case, users are prohibited from using IS&T resources to (non-exhaustive list):

- Download and store files, programs, codes, or software from unreliable Internet sources without the prior authorisation of ATR's Digitalisation Department;

- Download, store, install, uninstall, update, use or distribute software other than that provided or authorised by ATR;
- Download, store, or distribute non-professional material;
- Download, store, or distribute unauthorised material, protected by copyright and belonging to a third party;
- Consult and use “peer-to-peer” file sharing programs (for example, Torrent applications);
- Use any communication tool for professional purposes without prior authorisation from ATR's Digitalisation, Legal and/or HR Departments;
- Create independent websites or blogs on the Internet. All corporate information will be published on ATR's official website and managed by ATR's Communications Department.

Users are expressly prohibited from using IS&T resources, in particular to access the following content:

- Pornographic/paedophile/obscene;
- Racist, sexist, abusive or humiliating, including hate speech and publications whose content advocates the repression of certain groups and individuals (e.g. racial, religious, gender, sexual, age or disability minorities);
- Potentially insulting or defamatory;
- Degrading and/or discriminatory;
- Relating to obtaining, reselling, or consuming drugs;

- Promoting or inciting terrorism;
- Relating to the performance or promotion of criminal activities, such as instructions or references to methods/procedures to commit illegal acts;
- Referring to occult practices: publication of extremist views on occultism, Satanism, or similar subjects;
- Anonymous networks (such as TOR) or use of VPN services other than those used and authorised by ATR;
- Games (e.g. video games, online games, gambling, lotteries, etc.) and marketplaces (e.g. eBay);
- Content from any private social media or private email accounts for business purposes without permission from ATR.

Users are expressly prohibited from using the Internet/Intranet for the following purposes in particular:

- To expose ATR to penalties or embarrassing situations;
- To store ATR information on a public cloud or a private Internet storage service (for example, Dropbox, iCloud, or a personal server), unless this storage method has been formally authorised by the Digitalisation Department;
- To disclose information about ATR or refer to ATR on public websites, chats, forums, blogs, social media, or any other media, unless expressly authorised by the Communications Department.

5- MASTERED ATR PERSONAL COMPUTERS FOR SUBCONTRACTORS

ATR's subcontractors are given the option of accessing ATR's information system from a machine belonging to them.

5.1 PROVISION OF EQUIPMENT

In this particular case, the subcontracting company will then provide its employee with a machine in the format and technical specifications provided by the ATR Digitalisation Department (to be requested at the time). This machine will be configured by installing an ATR “master”, which will be done by the ATR

IT team, on our premises.

All the rules established in this document will apply to the use of these machines on the ATR information system.

5.2 DATA

All data created on the basis of a PC configured to the ATR standard will be the property of ATR and may be consulted and extracted at any time during the service.
The data are subject to the Storage and Retention rules of Article 8.2.

5.3 SOFTWARE

All of the software integrated via the ATR Master is the property of ATR.

5.4 END OF MISSION

At the end of the mission, the subcontractor will be required to complete an exit circuit in order to go through the ATR IT team, which will format the machine before returning it to the service provider.
In the event that this exit circuit is not carried out, the subcontractor undertakes to clean the PC containing ATR data.

6- IS&T MOBILE RESOURCES

ATR provides IS&T devices, such as smartphones, tablets, PCs, etc., to users (via the COD (Company Owned Device) model according to their needs, to allow them to access the ATR network for professional purposes and in accordance with Article 8.

7- CONFIDENTIALITY

Users will treat all information as confidential information, including facts, questions, documents, and any other data obtained in the performance of their professional duties at ATR.
Said confidential information will remain the property of ATR, its customers, its suppliers and/or its partners (as the case may be).
This duty of confidentiality will continue after the cessation or conclusion of the activities of the user with ATR, in accordance with the local laws, the contractual framework, or other regulations in force.

Users will not disclose or use any confidential information for purposes other than the performance of their professional/contractual responsibilities, unless expressly authorised by ATR.

Users must comply with the classification of information as defined by ATR and its Data Officers, who guarantee compliance with these rules, their distribution, and any amendments specific to certain Departments.

These rules are available on the following intranet page:
https://busservices.sharepoint.com/sites/ITS/SitePages/Classification-Factors-and-Sensitivity-Label.aspx
The list of Data Officers is available here: https://busservices.sharepoint.com/sites/ITS/SitePages/Data-

Officer.aspx .

8- SECURITY

8.1 AUTHENTICATION AND SECURITY MEASURES

Users will need to physically secure all their mobile devices such as laptops, removable media, mobile phones, tablets, etc., and ensure that they are handled properly to avoid theft or loss. In particular, they must never leave these devices unattended in public places or areas of ATR premises to which visitors have free access.

Users must log out or activate a password-protected screen saver when leaving their PC and mobile devices unattended, even for a short time.

Only removable media that have been approved or provided by the Digitalisation Department must be connected to IS&T resources.

Users must ensure the strict confidentiality of their passwords and access codes. No written record of this information should be kept; this information should also not be saved for automatic login purposes (for example, in a macro or a function key), unless these methods are validated by the Digitalisation Department. If a user suspects that an unauthorised person may have obtained their password or access codes, they must immediately change this information and inform the Helpdesk.

Users who have been provided with software to facilitate remote access authentication should protect these tools against loss or theft, and protect their PINs in the same way as their passwords.
Authentication and secure access tools should never be shared among multiple users. Users must notify their manager as well as the Digitalisation Department of the loss or theft of their authentication and secure access tools as soon as possible.

8.2 STORAGE AND RETENTION

All business data shall be stored by the user, for backup purposes, in the appropriate files/network storage of IS&T resources.

If a user encounters difficulties in storing professional data on a specific device or expresses special and justified requirements in terms of storage, they must contact the Digitalisation Department.

In case of accidental deletion of professional data, the user must immediately notify the local Helpdesk.

Subject to local laws and regulations, the use of IS&T resources (data communication) by all users may be recorded by ATR and stored for a period of one year (e.g. Internet browsing history).

As an Internet service provider for its employees (ISP), ATR may be required to provide the stored connection and usage data to the courts upon request.

9- MONITORING

9.1 PURPOSE AND SCOPE

ATR may monitor all activities involving IS&T resources.
Internet browsing on ATR networks will be filtered and monitored by ATR and/or external IT security tools in place.

This monitoring may lead to the deployment of various tools to protect the IS&T resources. These may include, for example, anti-virus programs, filtering mechanisms, and software to prevent data loss. ATR may also operate a computerised system to monitor secure communications (such as SSL-encrypted web traffic).

This monitoring is carried out for the following purposes:

- Ensure the confidentiality and integrity of ATR's infrastructures, networks, data, and IS&T resources;
- Ensure efficient use of IS&T resources and their normal operation;
- Ensure compliance with applicable laws and regulations and/or this document;
- Investigate any violation of applicable laws and regulations and/or this document;
- Ensure compliance by the user with the security and confidentiality obligations contained in this document;
- Identify, monitor, and protect ATR assets;
- Ensure effective cost control.

9.2 EXECUTION OF THE MONITORING

Monitoring activities must be carried out only by members of ATR's Digitalisation Department, who have received adequate training in terms of personal data protection.

For the purposes set out in Article 9.1 above, ATR may monitor any use of IS&T resources and access all professional data.
In this regard, ATR may monitor all activities involving the IS&T resources, including Internet browsing histories (names of websites visited, browsing time, files/material downloaded and bandwidth used, etc.), e-mails sent and received (including attachments), files stored on the IS&T resources (e.g. PST files), network connections, and any general logs relating to the IS&T resources.

In the event of a detection of a security incident, ATR may analyse the security measures applied (for example by carrying out a review of the relevant logs or an investigation of the IS&T resources) to identify the root causes of the incident and take corrective measures in order to limit the damage caused to the IS&T resources or to the interests of ATR.

In order to prevent and mitigate an imminent risk to the security of the IS&T resources or the interests of ATR, ATR may temporarily block or suspend the use of and access to the IS&T resources for a user.

9.3 ACCESS TO PERSONAL DATA AS PART OF MONITORING

Occasional use of IS&T resources for personal purposes is tolerated within the specified limits, however ATR may monitor all personal data (folders, e-mails, files and directories, whether identified as "Private", "Personal" or other) in accordance with the provisions of this document.

Users are advised that software deployed by ATR may not be able to distinguish between private and professional data. Users therefore acknowledge that monitoring activities apply equally to all data stored and transmitted via IS&T resources.

At the request of the Legal Department and/or the HR Department, the Digitalisation Department may, in compliance with the laws and regulations in force, access data identified as personal as specified in Article 2.2 in the event of reasonable suspicion of illegal use or when such access is necessary to prevent or mitigate an imminent risk or any event that harms or is likely to harm the security of ATR's IS&T resources or its interests.

10-PRIVACY AND DATA PROTECTION

Personal data is information that allows, directly or indirectly, to identify a natural person (examples: last name, first name, personal or professional telephone/e-mail number, salary, health data, etc.).

As part of its activities, ATR processes personal data. This processing (consultation, storage, recording, etc.) is carried out in accordance with the laws and regulations in force in terms of data protection, such as the European data protection regulation (GDPR no. 2016/679 of 14 April 2016) and the amended French Data Protection Act (Act no. 7817 of 6 January 1978).

In fact, each user may be required, as part of their missions, to process personal data. This processing must be carried out in accordance with the procedures established by ATR with regard to data protection and information security.

Each employee has the right to ask ATR for access to their data, the rectification or erasure thereof, or a limitation of processing as well as the right to oppose processing and the right to data portability.

These rights can be exercised by directly contacting the Data Protection Representative (DPR), guarantor and point of contact for the protection of personal data, by e-mail: data.protection@atr-aircraft.com.

In the event of the implementation of a new personal data processing or breach, or any attempted data breach, the DPR must be informed as soon as possible.

11-PENALTIES

If it is demonstrated that the non-compliance by a user with the provisions of this document is personally attributable to said user, subject to local laws and regulations, the following action may be taken by ATR:

- Disciplinary measures provided for in the rules of procedure;

and/or

Personal civil and/or criminal liability.

12-ENTRY INTO FORCE

This document was the subject of information and consultation by the Social and Economic Committee (CSE) on April 22, 2021, in accordance with the regulations. This document comes into force on 3 June

2021.

In order to comply with the laws and regulations in force and with any changes in ATR's policy, this document may be modified by ATR as often as necessary, subject to compliance with the national social procedures in force.

The latest version of this document will be published on the ATR Intranet and communicated on simple request addressed to the Human Resources Department.

APPENDIX 1 - GLOSSARY

ATR: refers to the ATR IEG as a company.

Document: this reference document, including its appendices, which defines the principles and procedures for using ATR's IS&T resources.

User: any person likely to use or have access to IS&T ATR resources. Users may be employees regardless of the type of contract (permanent, fixed-term, sandwich course), temporary workers, trainees, employees posted by LEONARDO or made available by AIRBUS ATR, subcontractors, service providers, customers, visitors, with access to IS&T resources. For clarification purposes, members of the IT department as well as all IT profiles are included in this definition.

Digitalisation Department: department within ATR responsible for providing IS&T resources to users.

IS&T Resources: refers to the Information Systems and Technologies provided by ATR (or by a service provider on behalf of ATR) to users in order to enable them to carry out their professional tasks. These resources include: PCs, laptops, removable media, phones, tablets and software, “professional containers” installed on IS&T resources owned by ATR or the user, as well as ancillary services and equipment, necessary to support and facilitate the ATR information system (e.g. security tools, CCTV image processing, and access control)

IP/network address: numerical address by which a location on the Internet is identified and which makes it possible to identify the user's computer on the network. ATR IP addresses on the Internet are fixed. Regardless of the IP address of their computer on the ATR network, any user connected to the Internet from ATR receives an Internet IP address belonging to ATR and identifies ATR as the source of the activity carried out.

Personal data: any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Untrusted Internet sources: refers to websites with questionable security certificates, in which case your Internet browser warns you that the website should be treated as an untrusted site.

Monitoring/monitor: Monitoring means all automated processes for filtering, sorting, and tracing flows and data passing through ATR's information systems. These processes, which involve an automatic and undifferentiated control of the files and their content, do not require the systematic viewing of the data by a natural person.

APPENDIX 2 - FAQs

Topics/Questions	Answers
Objectives of the Charter on IS&T resources	This Charter on IS&T resources aims to consolidate and harmonise the ATR rules relating to the use of IS&T resources by users. The consolidation of these rules in a common document has made it possible to clarify the conditions of use and to strengthen the protection of ATR and users, while ensuring the functionality of this Reference Document at the national level.
Why are "occasional private e-mails", "occasional private use of the Internet" or any "occasional private use of ATR's IS&T resources" allowed in some countries, but not in others?	As explained, this document has been drawn up in order to harmonise the rules related to the use of IS&T resources by users. As national laws regarding the use of IS&T resources differ from country to country, it is not always possible to take a comprehensive approach to all potential issues. In some countries, case law indicates that IS&T resources provided by an employer can be used for private purposes, provided that such use is reasonable and does not prevent employees from carrying out their work. In other countries, this is not allowed. ATR's Management has therefore decided, in compliance with national laws, to restrict the use of IS&T resources for private purposes as much as possible. The basic principle is that IS&T devices should not be used for non-professional activities, except for minor and exceptional use (e.g. in case of emergency or interruption while travelling, or for contacting friends and family). Users should adopt a common sense approach in their use of IS&T resources for private purposes.
In the event that a user is based abroad, but has a contract with an ATR entity based in their country of origin, how is the use of IS&T resources for private reasons governed?	The use of IS&T resources for private reasons is subject to the rules of the country of origin.

I work abroad and want to use IS&T resources to communicate with and support my family. Is it possible?	There is no specific right allowing the use of IS&T resources by employees for private purposes. However, courts are often willing to conclude that employees may make reasonable private use of IS&T resources provided by the employer, provided that such use does not interfere with their professional duties. Employers are not required to allow employees to use communications equipment for private purposes. However, many employers choose to do so. In order to ensure the integrity and confidentiality of the system, the ATR Management has decided to prohibit employees from using IS&T resources for private purposes in certain countries, namely, countries where such a prohibition is authorised.
Do the provisions of the IS&T charter apply when these are used outside working hours to access non-professional websites?	The stipulations of the charter on IS&T resources are applicable to all IS&T resources, whether they are used in the office, at home, in a hotel, etc.
How do I know which documents are confidential?	The rules are available on the following intranet page: https://busservices.sharepoint.com/sites/ITS/SitePages/Classification-Factors-and-Sensitivity-Label.aspx The list of Data Officers is available here: https://busservices.sharepoint.com/sites/ITS/SitePages/Data-Officer.aspx .
Where should I store my archives when my standard disk is full?	In accordance with Article 7.2 above, all professional data must be stored on the hard disk of the device receiving or creating the data. If you are having difficulty storing your professional data, you should contact the Digitalisation Department as soon as possible.

ATR EIG

CODE OF CONDUCT

MESSAGE FROM OUR CEO

Dear colleagues,

As a world leader in the regional aircraft market, ATR must set an example in all its fields of activity. Leading by example is even more essential when it comes to Ethics and Compliance. In this respect, we aim to apply the highest standards of moral values and ethical principles at all times in our work, both in our relations with the outside world and within our organisation.

To ensure this commitment, Ethics and Compliance are among ATR's priorities this year, alongside our operational and commercial objectives.

While these operational and business objectives are indeed of the utmost importance, how to achieve them is just as crucial as achieving them. In order to continue to be the leader in our market, we must preserve our reputation and the brand image, which will only be possible through the highest level of requirements in terms of Ethics and Compliance. It cannot be enough to avoid penalties and fines resulting from inappropriate and immoral conduct. We must place our ethical principles at the core of our daily work at ATR.

This is why ATR has adopted a zero tolerance policy against illegal practices and corruption. Under no circumstances will acts that undermine our values or violate applicable rules be tolerated.

As part of our Ethics & Compliance programme, the Legal Department has established and maintains a set of principles, guidelines, and procedures. They include: the ATR Integrity Principles, the Conflict of Interest Directive, the Sponsorship & Donations Policy for sponsorship and donation projects, the Offer and Acceptance of Gifts/Benefits Directive, the Business Development Anti-Corruption Policy, which contains best practices for ATR's business development, and the Export Compliance Directive, which contains rules and procedures to ensure compliance with export control laws and regulations.

Regular training in this area will also help us understand, adopt, and defend our values of integrity in the world. These trainings will enable each employee of ATR and its subsidiaries to adhere to and share these principles.

To summarise, I am counting on each and every one of you to keep our values of ethics and integrity alive. This collaboration must be based on a bond of trust and respect in our relations with our points of contact (customers, suppliers, institutions, and other parties), thus contributing to ATR's status as the undisputed leader in the regional aviation market.

Christian Scherer

This Code of Conduct identifies the key principles and values that every employee, trainee, external employee (temporary workers, subcontractors, etc.), director and manager of ATR, as well as of each of the entities controlled by ATR (hereinafter ATR subsidiaries), must apply and respect in their day-to-day work in order to make integrity and compliance a reality and a part of our corporate culture.

This Code of Conduct has been adopted by the Assembly of Members and constitutes one of the pillars of ATR's Ethics & Compliance programme.

This Code of Conduct refers to the guidelines and documents currently in force, which provide detailed instructions for certain specific issues. These guidelines and documents are available on the ATR intranet as well as on the ATR quality portal.

This Code of Conduct and the documents referred to in it will not necessarily provide a solution to all the specific situations that you may face. Therefore, if in doubt, you are strongly recommended to seek advice or raise any concerns with your management, the Human Resources Department, the Ethics & Compliance team or via the OpenLine system available on the ATR intranet.

Any breach of our compliance rules may give rise to civil and/or criminal proceedings against ATR and its affiliates, and against the persons involved. Such persons will also be subject to appropriate disciplinary action. It is our responsibility to maintain and nurture an "ethical" culture based on "Speak Up".

CONTACT PERSONS FOR COMPLIANCE MATTERS

To make any suggestions, ask any questions, or obtain assistance in the interpretation and application of this Code of Conduct, you can contact the ATR Ethics & Compliance team, who will provide you with their support and assistance:

Email address: Compliance@atr-aircraft.com

Tel.: +33 (0)5 62 21 65 16

1. OUR WORK ENVIRONMENT

EMPLOYEES

ATR is aware of the need to create a pleasant working environment in which interactions with our employees, customers, suppliers, and other stakeholders are guided by principles of equality, fairness, respect, solidarity, integrity, honesty, and transparency.

ATR is committed to applying the highest standards of health, safety, and security in the workplace. At all times, we must comply with all applicable health and safety laws, policies, and internal procedures.

Each person is hired and promoted based on their qualifications, potential, performance, behaviour, and willingness to work in different positions and within different entities.

ATR is committed to the continuous development of its employees, regardless of their position in the company, by encouraging them to participate in regular awareness sessions and training.

ATR values diversity of ethnicity, gender, religion, citizenship, national origin, political opinion, sexual orientation, social background, age, and physical or mental characteristics.

No form of discrimination or harassment, whether physical, visual or verbal, will be tolerated.

What is harassment?

Broadly speaking, "harassment" is any type of behaviour that has the purpose or effect of violating the dignity of a person and of creating an intimidating, hostile, degrading, humiliating or offensive work environment.

EXPRESS YOURSELF

ATR is committed to creating an environment of trust conducive to open and constructive dialogue between colleagues and with the Management.

ATR will not tolerate any form of retaliation or attempted retaliation against persons who have expressed, in good faith, concerns or provided assistance in the context of investigations into alleged violations of the law, this Code of Conduct, or any related document.

Employees wishing to raise a concern, seek advice or submit a complaint can contact their manager, the Human Resources Department or the Ethics & Compliance team or use the OpenLine tool available at www.airbusgroupopenline.com. All reports and queries will be kept confidential and will be investigated thoroughly as soon as possible. Feedback on the results of the investigation will be provided in due time.

2. PROPERTY AND INFORMATION

PROTECTION OF PROPERTY

We must protect ATR's property, such as equipment, tools, facilities, supplies, software, data, and information and telecommunication systems so that none of them are stolen, damaged, misused, or improperly destroyed.

We must use and treat all ATR property entrusted to us in a safe, ethical, legal, and productive manner, as if it were ours. ATR's property must only be used for the purposes of achieving ATR's business objectives and must not be used in any unlawful or improper manner.

In our day-to-day business, we must always take care to secure and protect ATR's intellectual property and avoid infringing the intellectual property rights of third parties.

Reference documents:

- Instructions and behaviour guidelines for sound management of the company's assets

- ATR charter for the secure use of information and communication systems

What is ATR property?

• Physical assets such as facilities, equipment, tools and inventory, securities and cash, office equipment and supplies, information systems and software;

• Confidential and private information, including information that has not yet been made public and internal business information, such as documents related to contracts, business processes, corporate strategies, and operating plans;

What is intellectual property?

Creative ideas and works of the human mind with commercial value such as patents, trademarks, copyrights, "know-how", technical information, and any other form of unregistered intellectual property.

KEEPING ACCURATE RECORDS

Our associates, business partners, government authorities, and all interested parties rely on the accuracy and correctness of the information provided by ATR. It is therefore our responsibility to ensure that the information we provide to these parties is accurate, complete, and understandable to all.

We must maintain our financial records in strict compliance with applicable laws and regulations, as well as our internal control procedures. Employees must not create or participate in the creation of records that contain misleading information or conceal inappropriate activities.

PROTECTION OF PERSONAL DATA AND CONFIDENTIAL INFORMATION

ATR collects, processes, and uses the personal data of its employees, partners, and other relevant parties. In this context, ATR complies with the applicable laws and regulations.

Customers, suppliers, government authorities, and other relevant parties frequently entrust ATR with their own confidential and private information. We must handle such confidential or private information of third parties in accordance with the terms of its disclosure and in strict compliance with all applicable laws and regulations.

Access to confidential and private information is strictly limited to those who really need to know it. This information may be disclosed only to officially authorised employees or external stakeholders who need the information for legitimate business purposes or if disclosure is required by law. Prior to the transmission or receipt of any confidential information by any business partner, an ATR Confidentiality Agreement should be signed.

We must refrain from accepting, requesting, or disclosing private or confidential information from third parties without having obtained the owner's consent to their transfers. The Legal and Compliance Department must be promptly informed of the receipt of any confidential or private information from third parties received without authorisation.

COMMUNICATION MANAGEMENT

ATR's reputation and image must be protected and promoted at all times with the help of the Communication Department.

All public statements, disclosures of information or responses to media inquiries must be approved by the appropriate persons within ATR's Communications Department.

The Communications Department is responsible for managing ATR's image, its presence on social media, and all matters related to communication.

We must not act on behalf of ATR by sending information to the media or by intervening on social media. We must direct all questions and requests for information from the media to the Communications Department.

Disclosed information and the content of published materials, such as brochures, advertisements, and editorial help documents must be accurate and must not disparage the products, services, or employees of our competitors.

3. BUSINESS PRACTICES

ZERO TOLERANCE FOR CORRUPTION

Corruption and influence peddling of any kind, whether involving public or private entities or natural persons, are strictly prohibited. Therefore, we must never:

- offer, attempt to offer, give, authorise or promise a bribe (i.e. anything of value), facilitation payment or kickback of any kind to any natural or legal person in order to obtain or retain business or any improper advantage.

- solicit, receive or accept a bribe, facilitation payment or kickback from any natural or legal person.

Specific laws and regulations apply to dealings with government officials and their family members. We must therefore be extra vigilant when interacting with public officials and their family members. We should never hire someone else to do something that ethics or the law does not allow us to do ourselves. The Business Development Anti-Corruption Policy applies to all business development activities involving third parties.

We must not wilfully ignore or overlook any acts of corruption or influence peddling. It is everyone's responsibility to ensure that these rules are respected by each of us.

Exceptionally, facilitation payments may be tolerated if they are made for the purpose of protecting a person's health, safety, or well-being. In such a case, the ATR Ethics and Compliance team should be contacted immediately.

Q&A

QUESTION: You meet an airline representative who asks if their son can do an internship with ATR. How should you react to this proposal?

ANSWER: You should treat this request with caution as an internship offer is likely to be considered a benefit. Therefore, explain to the representative that you are not looking for interns, but that their son can submit their application following the usual ATR recruitment procedure.

QUESTION: A supplier participates in a call for tenders organised by ATR and offers you a gift in exchange for your positive recommendation during the selection process. How should you react to this proposal?

ANSWER: This proposal must be rejected, documented, and reported to ATR's Ethics & Compliance team.

QUESTION: To maintain good business relations with a customer, you want to offer him a box of chocolates for the New Year. Is this acceptable?

ANSWER: Yes, provided it is a low value gift given at a time when gifts of this nature are commonly exchanged. For additional information on the exchange of gifts and benefits, please refer to the applicable guideline.

QUESTION: You want to organise a training session for the representatives of a client located abroad. At the end of the training, the head of the delegation asks you to organise a weekend in a prestigious hotel in Naples.

ANSWER: This proposal should be politely but firmly rejected as accepting it could jeopardise their independence, as well as ATR's reputation, as its purpose is primarily recreational and its value is excessive, which is against ATR policy. However, you can help them, for example by indicating establishments in which they can stay or by making a reservation in a hotel if they do not speak Italian.

QUESTION: A former member of a local government is considering consulting assignments for ATR and says he will use his connections in government to obtain the necessary administrative approvals to expand ATR's operations in that country.

ANSWER: The payment of a sum of money to a person so that they use their influence within a public authority to obtain a favourable decision falls under influence peddling, which is strictly prohibited. It is therefore desirable to exercise particular vigilance for consulting assignments and to ensure their legality with the assistance of the ATR Ethics & Compliance team.

QUESTION: You are due to travel abroad in two weeks and therefore need to obtain a visa urgently. At the embassy, the public official tells you that you will get your visa in a month, but offers to speed up the procedure for a 50 euro note. How should you react to this proposal?

ANSWER: This type of practice falls under facilitation payment and is therefore prohibited. You must therefore refuse any such arrangement, regardless of the amount, and inform your management of the delay.

What is bribery?

Promising to offer or giving, soliciting or receiving - directly or indirectly - any undue advantage of a financial or other nature to or from another person in such a way that person, in breach of their duties, acts or refrains from acting in order to obtain or retain business or other undue advantage.

What are facilitation payments?

Secret payments of limited value made to lower-level public officials to expedite or obtain the execution of routine administrative processes.

What is influence peddling?

This is the practice of offering, directly or indirectly, donations, promises, invitations, gifts or advantages of any kind to a public official or private individual in order for that person to use their actual or presumed influence to obtain authorisations, employment, a public contract or any other favourable decision from a public authority, whether national or foreign.

Reference document:

- Business Development Anti-Corruption Policy Directive

MANAGEMENT OF GIFTS AND BENEFITS

ATR acknowledges that in the course of successful and lasting business relationships, gifts or benefits may be exchanged on certain appropriate occasions. However, if given in inappropriate circumstances, gifts or benefits may be interpreted as an attempt to exert undue influence on the recipient. This risk exists whether the gift or benefit is given or received and whether the third party is a public official or works in the private sector.

Those in a position to exchange gifts or benefits with third parties should carefully analyse each situation to ensure that the gift or benefit being considered, whether given or received, is ethical, legal and complies with the requirements of the Gifts and Hospitality Directive.

To ensure full transparency, any gift or benefit given or received must be fully and accurately recorded using the template available on ATR's intranet and approved if required by the applicable directive.

Reference documents:

- Gifts & Hospitality Directive

- Gifts & Hospitality Country list

- Gifts & Hospitality Recording & Approval Form

IDENTIFICATION AND MANAGEMENT OF CONFLICTS OF INTEREST

ATR is committed to placing the interests of the company above any direct or indirect personal interest and therefore ensures that all decisions are based exclusively on the merits of each option.

We must in all circumstances avoid actual and potential conflicts of interest because they may influence our judgement, our objectivity, or our loyalty to ATR.

Conflict of interest situations, which may arise at any time, are not condemnable per se, but must be declared and managed in accordance with the Directive and the procedures applicable to conflicts of interest.

We must exercise particular vigilance when we engage former or current public officials or civil servants as employees, consultants, or subcontractors.

What is a conflict of interest?

A conflict of interest arises when our personal interests interfere, or appear to interfere, with our ability to perform our duties impartially in the interests of ATR. For example, a conflict may arise when an employee, family member, relative or friend has an undisclosed financial interest in a customer, supplier, partner, or competitor of ATR.

Reference documents:

- Conflict of Interest Directive

- Conflict of Interest Declaration Procedure

- Conflict of Interest Declaration Form

FIGHT AGAINST MONEY LAUNDERING

ATR deals exclusively with reputable clients who are engaged in legitimate business activities and whose funds are derived from legitimate sources.

Therefore, before entering into a business relationship, ATR will carry out a prior verification of the customer known as *Know Your Customer* (KYC).

What is money laundering?

It is the process by which a person or company passes off illegally obtained ("dirty") money as legitimate ("clean").

FAIR COMPETITION

We must strictly comply with applicable competition law in the countries in which we operate. Competition law prohibits agreements or conduct that may restrict or affect competition or trade.

We must take extra care when exchanging or disclosing commercially sensitive information about competitors, customers, or suppliers, particularly in the context of calls for tenders. If in doubt, you can contact the Legal and Compliance Department.

Reference document:

- Antitrust Do's and Don'ts

IMPORT AND EXPORT CONTROL

ATR buys and sells products and services to a large number of customers and suppliers located around the world. It is therefore essential that each import and export is monitored to ensure compliance with all applicable laws and regulations governing such activities.

The Ethics & Compliance team is available to answer any questions or concerns regarding the import or export of products, services, or information.

What is an "Export"?

An export occurs when products, services, technology, or software are transferred to another country or when products, services, technology, or software are transferred to a foreign person or company, wherever located. Export occurs when the transfer is made verbally, by e-mail, by post, by hand delivery, or by a server, etc.

Reference document:

Export Control Directive

RELATIONS WITH RELEVANT PARTIES

In the course of its activities, ATR regularly cooperates with national and international authorities on a wide range of issues such as export licensing or aircraft certification. In our interactions with these authorities, we must ensure that all matters are handled professionally, in a timely manner, and in accordance with the law. Any inquiry or request for information from these authorities must be handled in coordination with the General Secretariat and the Legal and Compliance Department.

It is the responsibility of the Purchasing Department to ensure that ATR's relations with its suppliers are managed fairly and in accordance with the law. We must ensure that our relationships are formalised in the best possible manner and that the selection of each supplier is based exclusively on the merit of each offer.

ATR strives to source responsibly from suppliers with the highest standards of integrity. ATR must ensure that those in its supply chain comply with all applicable laws and regulations, apply the highest standards of health and safety, and adopt principles of integrity similar to its own. Suppliers may therefore be asked to provide proof of their commitments, particularly in the areas of business ethics, anti-corruption, human rights (e.g. anti-trafficking, anti-child labour), labour standards, and environmental sustainability.

ATR conducts business with trusted stakeholders who adhere to the highest principles of integrity. Therefore, before entering into a business relationship, ATR will conduct due diligence on any stakeholder, which may include Know Your Customer (KYC) and Know Your Supplier (KYS) procedures.

SAFETY AND QUALITY

In order to meet its commitment to product quality and safety to its customers, ATR must adhere to the highest standards of safety and quality control, all internal control policies and procedures, and all applicable laws and regulations. Product quality and safety are the top priority and must continue after the product is delivered.

We must continually keep the safety of our products and services in mind, while maintaining the highest safety standards. Product safety is highly dependent on the information and feedback provided and we are therefore strongly encouraged to immediately forward any safety reports, concerns, or information. We are dedicated to ensuring that our products are designed, manufactured, delivered, and repaired as per the highest safety standards.

We must constantly develop and strengthen all activities related to quality, because excellence in this area is our top priority. Each of us must be aware of our role and responsibilities with regard to quality throughout the product life cycle. We must report, stop, and fix any problem we may see.

Reference documents:

- Flight Safety Policy

- Flight Safety Voluntary Reporting Process.

- Quality Policy

4. SOCIAL RESPONSIBILITY

SUPPORTING OUR COMMUNITIES

As a leader in the regional aviation market, ATR acknowledges that it has a responsibility to the aviation industry, local communities, innovation, education, the environment, and sustainable development, and strives to make valuable contributions in these areas.

ATR can therefore contribute in these areas by making donations or by sponsoring events, conferences, foundations, institutions, etc. Any membership in an organisation, association, society, club, etc. will be considered as sponsorship.

All sponsorships and donations must be conducted in accordance with relevant internal policies and all applicable laws and regulations. These initiatives must be transparent, approved and accurately recorded, must fall within one of ATR's sponsorship and donation strategic areas, and must be consistent with ATR's brand positioning.

ATR must not participate in the financing of organisations or political parties and religious organisations. ATR shall also not provide goods, services, or any other benefit to such organisations or parties.

Reference documents:

- Sponsorship & Donation Directive

- Sponsorship & Donation Procedure

ECO-EFFICIENCY OBJECTIVE

As an environmentally responsible company, ATR is committed to eco-efficiency in all its business activities, including efforts to reduce the environmental impact of the products and services it delivers.

In addition to complying with all applicable laws, regulations and internal policies relating to the protection of the environment, ATR recognises its responsibility to raise awareness about environmental issues in the aviation industry.

At all times, we should ensure that we do everything we can to reduce our impact on the environment, starting with low-effort measures such as turning off the lights when leaving the office or printing only when necessary.

What is eco-efficiency? Eco-efficiency is about maximizing the benefits of the products and services we provide to our customers and other relevant parties while minimising the impact of these products on the environment throughout their life cycle.

Reference documents:

- ATR's Environmental Objectives

- 2021 Environmental Vision

- ISO 14001 Certification