



SAFETY POLICY

In my capacity as accountable manager, I consider that both operational and information security in all areas and services of CLIPPER NATIONAL AIR is one of our basic functions to be implemented and maintained effectively, and, considering the size, nature, and complexity of our Company, I commit myself and involve all those in charge to:

1. Comply with applicable regulation (Part IS.I, Part 145, Part CAMO, and Part ORO), consider relevant standards and best practices.
Each manager in their area should continuously promote the Safety Policy among their employees, value acceptable behaviors, and correct those that are not, in accordance with the provisions of our manuals.
2. Communicate this policy to all staff, both in-house and subcontracted, through the established communication channels (email, website, office signage, among others) and ensure that it is understood by including it in training sessions, and that it is implemented and maintained by checking it during internal supervisions, audits, or inspections.
3. Identify both operational and information security as the Company's highest priority, above commercial, operational, environmental, or social pressures.
4. Review this Policy annually as part of the Management System review process, or whenever a change occurs that involves a significant alteration or modification with a significant impact on the organization's operations, in order to ensure that it remains relevant and appropriate to the Company, maintaining our commitment to improvement towards the highest safety standards.
5. In relation to the Part 145 maintenance organization, commitment to the application of human factors principles, including due consideration to fatigue aspects.
6. Establish objectives and performance measures for information security management;
7. Define general principles, activities, and processes for the organization to adequately protect information and communication technology systems and data;
8. Apply the ISMS requirements to the organization's processes;
9. Continuously improve toward higher levels of maturity in information security processes;
10. Comply with applicable requirements regarding information security and its proactive and systematic management, and provide adequate resources for its implementation and operation;
11. Assign information security as one of the essential responsibilities of all key personnel.
12. Promote the information security policy through training or awareness sessions within the organization for all staff on a regular basis or prior to changes.
13. Promote periodic event reporting, with a confidential reporting system to capture events, ensuring the anonymization of the source, feedback, and the recording of events in a database, considering that this is an important source for identifying hazards in our management system.



14. The procedures established in MSG 3.2.1.4 for mandatory or voluntary reporting of events shall be applied, and an internal safety investigation shall be conducted for those events that correspond to the provisions of the procedure.
15. Work toward continuously improving safety levels, complying with applicable legal requirements and standards, applying best practices, providing the necessary resources, and making safety one of everyone's primary responsibilities.
16. The purpose of notifications and investigations shall never be to find someone to blame, but rather to improve safety.
17. Actively encourage effective safety reporting and distinguish between acceptable behavior (unintentional errors), for which no disciplinary action will be taken, and unacceptable behavior (recklessness, negligence, sabotage, etc.), for which action may be taken once those responsible have been identified (just culture).



Firmado digitalmente
por 33963573W
DANIEL MARTINEZ (R:
A60344546)
Fecha: 2026.01.27
12:24:16 +01'00'

Daniel Martínez Téllez
Accountable Manager