

## INFORMATION SECURITY POLICY

Information and information system protection are the main objectives of THALES HELLAS.

Our company's management commits in supporting any action aiming to the elevation of the corporate information security performance. For this reason, the company takes the proper technical and organizational measures to ensure the availability, integrity and confidentiality of the data it processes.

THALES HELLAS has developed an Information Security Management System aiming to:

- Ensure the integrity, availability and confidentiality of its IT systems
- Handle promptly and effectively any information security incidents that threaten its normal operation
- Continuously improve the Information Security performance
- Comply with legal and regulatory requirements, including GDPR.

In order to support the aforementioned objectives, our company developed:

- Organizational roles required for monitoring the Information Security performance
- Information classification scheme. All information is classified, based on its importance and criticality, according to corporate information classification method.
- Technical measures for protecting, controlling and restricting access to information and information systems.
- Information Security incident reporting and handling method, to handle in time and effectively security incidents.
- Training methods to keep all our employees informed in the cutting-edge security threats.
- Key Performance Indicators to measure and monitor critical factors which designate the corporate security level.
- Methods for ensuring the continuous operation of business processes in case of information systems failures or physical disasters.
- Risk assessment method in order to identify the threats and vulnerabilities our company is exposed to. This helps us to evaluate our risk level exposure and to determine appropriate control implementation.
- Continuous improvement and maintenance of our IT Systems.

The Information Security Officer is responsible for the Information Security Management System operation and control as well as for taking the required initiatives to eliminate any factor that may lead to company's information availability, integrity or confidentiality compromise.

Company's employees and partners with access to information and information systems are responsible for adhering to the rules of the implemented Information Security Policy.

Company's management and employees are committed in continuous improvement of the corporate Information Security Management System.

**DEFRANOUX Patrick**  
*Chairman and C.E.O.*  
08<sup>th</sup> January, 2024

