

***RFC 2350***

***LDO-CERT***

Copyright LeonardoS.p.A. All rights reserved.

The contents of this document, owned by Leonardo S.p.A., are confidential and are provided without liability for errors and omissions. It is forbidden any reproduction, distribution and use, even partial, in the absence of formal written permission of Leonardo S.p.A. The copyright and this use restriction must be considered extended to any form or display mode of the information here contained.

# Document Information

## About This Document

This document contains a description of Leonardo Computer Emergency Response Team, which will referred as LDO-CERT, in according to RFC 2350. It provide basic information about the LDO-CERT team, its channels of communication, its roles and responsibilities.

## Date Of Last Update

Version 1.0, updated on 2017/10/31.

## Location Where This Document May Be Found

The current and latest version of this document is available on LDO-CERT website.

Its URL is <https://www.leonardocompany.com/cert>.

## Authenticating This Document

This document has been signed with the PGP key of LDO-CERT.

The public PGP key is available in LDO-CERT website.

## Document Identification

Title: RFC 2350 – LDO-CERT

Version: 1.0.

Document Date: 2017/10/31

Expiration: this document is valid until it is replaced by a later version.

# Contact Information

## Name Of The Team

Full Name: Leonardo Computer Emergency Response Team

Short Name: LDO-CERT

## Address

Postal Address: LDO-CERT, Via Faustiniana, 29, 00131, Rome, Italy.

## Time Zone

Central European (GMT+0100 and GMT+0200 from the last Sunday of March to the last Sunday of October).

## Telephone Number

Tel: (H24/7 365 day) +39 06 87972171.

## Electronic Mail Address

LDO-CERT can be reached via [cert@leonardocompany.com](mailto:cert@leonardocompany.com) or via PEC to [cyberdefence@pec.leonardocompany.com](mailto:cyberdefence@pec.leonardocompany.com). All members of LDO-CERT Team can read messages sent to this address.

## Public Keys And Other Encryption Information

In order to guarantee the security of communications the PGP technology is supported. LDO-CERT public PGP key for [cert@leonardocompany.com](mailto:cert@leonardocompany.com) is available on the public PGP key servers and in LDO-CERT website.

The key shall be used whenever information must be sent to LDO-CERT in a secure manner.

## Staff Members

LDO-CERT’s Team Leader is the CERT Manager. The team consist of Incident Management Team Leader, Incident Handlers, Threat Intelligence Team Leader, Threat Analysts, Laboratory Team Leader Specialist and Laboratory Specialists.

# Other Information

General information about the LDO-CERT can be found at LDO-CERT website: <https://www.leonardocompany.com/cert>.

## Point Of Costumer Contact

The preferred method for contacting LDO-CERT is by mail: [cert@leonardocompany.com](mailto:cert@leonardocompany.com).

The mailbox is checked 24h/7days.

The use of PGP is required to send confidential or sensitive information.

If is not possible to contact LDO-CERT via e-mail for security reasons, the contact may take place via telephone.

## Charter

### Mission Statement

The LDO-CERT mission is to support and protect Leonardo’s Group cyberspace from potentially critical cyber threats having concrete possibility to compromise company operational capability or to pose a serious threat to information security.

### Constituency

The constituency of LDO-CERT refers to all the legal entities in Leonardo Group with primary focus on the Italian boundary.

### Sponsorship And/Or Affiliation

LDO-CERT maintains contacts with various national and international CSIRT teams, with FIRST and Carnegie Mellon University according to its needs and the information exchange culture that it values.

### Authority

The establishment of the LDO-CERT was mandated via Company directive on 2017.04.07

## Policies

### Type Of Incident And Level Of Support

LDO-CERT manage and address unknown type and critical information security incident which occur or threaten to occur in its constituency. The level of support given by LDO-CERT will vary depending on the severity of the incident, the related Leonardo ICT assets impacted and the LDO-CERT resources at the time.

### Co-operation, Interaction And Disclosure Of Information

LDO-CERT highly considers the importance of operational coordination and information sharing among CERTs, CSIRTs, SOCs and similar bodies, and also with other organizations, which may aid to deliver its services or which provide benefits to LDO-CERT.

LDO-CERT also recognizes and supports the ISTLP (Information Sharing Traffic Light Protocol).

### Communication And Authentication

LDO-CERT protects sensitive information in accordance with relevant local regulations and policies. In particular, LDO-CERT respects the sensitivity markings allocated by originators of information communicated to LDO-CERT ("originator control"). Communication security (which includes both encryption and authentication) is achieved using PGP primarily or any other agreed means, depending on the sensitivity level and context.

# Service

## Incident Management

The LDO-CERT performs incident handling, response on-site, support and coordination for its constituency. The incident management services as developed by LDO-CERT covers all “5 steps”:

* Preparedness and prevention
* Detection
* Analysis
* Response
* Recovery

## Threat Intelligence

The LDO-CERT performs the threat intelligence services in order to improve prevention, detection, identification and information security incidents response capabilities and strength the Leonardo cyber security posture.

# Incident Reporting Form

LDO-CERT does not provide any incident reporting form in a public web page. Please report security incidents via encrypted e-mail to [cert@leonardocompany.com](mailto:cert@leonardocompany.com).

Please classify the information using the Traffic Light Protocol and make sure to always include your own contact information.

# Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, LDO-CERT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.