NOTICE

DISCLAIMER. The information contained in this publication is subject to constant review in the light of changing government requirements and regulations. No subscriber or other reader should act on the basis of any such information without referring to applicable laws and regulations and/or without taking appropriate professional advice. Although every effort has been made to ensure accuracy, the International Air Transport Association shall not be held responsible for any loss or damage caused by errors, omissions, misprints or misinterpretation of the contents hereof. Furthermore, the International Air Transport Association expressly disclaims any and all liability to any person or entity, whether a purchaser of this publication or not, in respect of anything done or omitted, and the consequences of anything done or omitted, by any such person or entity in reliance on the contents of this publication.

Opinions expressed in advertisements appearing in this publication are the advertiser’s opinions and do not necessarily reflect those of IATA. The mention of specific companies or products in advertisement does not imply that they are endorsed or recommended by IATA in preference to others of a similar nature which are not mentioned or advertised.

© International Air Transport Association. All Rights Reserved. No part of this publication may be reproduced, recast, reformatted or transmitted in any form by any means, electronic or mechanical, including photocopying, recording or any information storage and retrieval system, without the prior written permission from:

Senior Vice President
Airport, Passenger, Cargo and Security
International Air Transport Association
800 Place Victoria
P.O. Box 113
Montreal, Quebec
CANADA H4Z 1M1
# Table of Contents

## Foreword

Chapter 1—Introduction

Chapter 2—Management

  2.1 SeMS Implementation Overview
  2.2 Corporate Commitment
  2.3 Authorities, Accountabilities and Responsibilities
  2.4 Security Objectives and Security Performance Standards
  2.5 Security Culture
  2.6 Provision of Resources
  2.7 Security Department
  2.8 Security Communication

Chapter 3—Documentation

  3.1 Aircraft Operator Security Program
  3.2 Security Reporting

Chapter 4—Aviation Security Quality

  4.1 Quality Assurance and Quality Control
  4.2 Quality Assurance Audits
  4.3 Quality Control
  4.4 Security Audits
  4.5 Security Surveys
  4.6 Security Tests
  4.7 Security Exercises

Chapter 5—Security Risk Management

  5.1 Security Risk Assessment
  5.2 Threat Identification and Assessment
  5.3 Risk Management Process
  5.4 Operational Risk Assessment

Chapter 6—Additional Guidance

  6.1 Role of Regulations, Regulators and Regulated Entities
  6.2 SeMS Dashboard and SeMS Implementation Plan
  6.3 Landside Security
  6.4 Insider Threats
  6.5 In-Flight Theft
  6.6 Application of SeMS to Cyber Management Framework
  6.7 Application of Risk Management Concepts to Cyber Threats and Risks

2ND EDITION, OCTOBER 2018
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.8</td>
<td>Recognition of Equivalence</td>
<td>183</td>
</tr>
<tr>
<td>6.9</td>
<td>Case Study–Aviation Security Culture–United Airlines</td>
<td>190</td>
</tr>
<tr>
<td>6.10</td>
<td>Case Study–Overflying Conflict Zones–LOT Polish Airlines</td>
<td>197</td>
</tr>
<tr>
<td>6.11</td>
<td>Case Study–Qantas Group Cyber Management Model</td>
<td>199</td>
</tr>
<tr>
<td></td>
<td>Acronyms</td>
<td>203</td>
</tr>
</tbody>
</table>