国 际 民 用 航 空 组 织

工 作 文 件

HLCAS/2-WP/19
16/10/18

第二次高级别航空安保会议（HLCAS/2）

2018年11月29日至30日，蒙特利尔

议程项目2：未来管理航空安保风险的方法

促进安保文化

（由比利时、加拿大、德国、意大利、新西兰、葡萄牙、卡塔尔、罗马尼亚、新加坡、瑞士、联合王国、美国和国际机场理事会提交）

摘要

建立全面的安保文化对于长期有效的航空安保至关重要。为配合全球航空安保计划（GASeP）的优先目标，国际民航组织航空安保专家组（AVSEC专家组）培训工作组（WGT）与国际民航组织秘书处合作，正在采取行动推广安保文化的重要性、并增进国际民航组织向成员国提供安保文化指导和培训的能力。

航空安保高级别会议的行动在第4段。

1. 引言

1.1 国际民航组织全球航空安保计划（GASeP）的优先成果 2 侧重于培养安保文化和人员能力。安保文化是一组规范、信念、价值观、态度和假设，是组织日常运作所固有的，并且反映在组织内所有实体和人员的行动和行为中。在航空安保方面，建立强大的安保文化将优化利用共享资源，促进信息共享，以确保承认有效安保对业务成功至关重要、将制定员工的积极安保做法作为核心价值，并使安保与核心业务目标保持一致。 航空安保专家组的培训工作组完全支持这一关键成果，并指出建立和维持强大而稳健的安保文化以及发展人力资本、技能和能力的重要性。

1.2 培训工作组欢迎全球航空安保计划优先成果 2 项下的以下任务：

2.A 审查或编制培训材料，教授安保文化及其原则。

2.B 制订安保意识方案，有效促进一个积极的安保文化。

2.C 继续推进安保意识宣传活动。

2.E 制订并向其它所有利害攸关方传达宣传计划、报告工具、推广材料和示范培训。

2.F 制定宣传战略，建立大众对航空安保以及遵守安保措施的重要性的意识。

2. 培训工作组为促进安保文化已采取的行动

2.1 培训工作组经与国际民航组织秘书处合作，在其正式工作计划下开展了实现全球航空安保计划中关于安保文化任务的工作。2017 年，培训工作组制作了加强安保文化工具包(附录 A)，旨在帮助航空业组织加强强有力的安保文化，以建立有效的安保制度。该工具包概述了许多工具，以支持教员和管理人员在员工队伍中深植和维持强大的安保行为。

2.2 培训工作组还一直在制定关于加强积极安保文化的讲习班。该讲习班将侧重于业界的高中级管理人员以及负责实施安保措施的其他人员，目的是通过及早发现潜在的安保挑战，帮助他们建立积极的安保文化并提高其整体安保绩效。讲习班的大纲在 2018 年 7 月的培训工作组会议上定案。

2.3 在努力提高安保文化意识方面，培训工作组与国际民航组织秘书处合作，作为 2018 年国际民航组织航空安保专题讨论会活动的一部分，开展了安保文化研讨会。本次研讨会为参与者提供了关于制定行为改变运动和工具的最佳做法，以在其组织内实施积极的安保文化。

3. 加强积极的安保文化

3.1 有效的安保文化可促使员工参与安保问题并对其负责。这是保护性安保制度的重要组成部分，用于支持和维护具有风险抵御能力的组织。促进积极的安保文化有助于减轻内部人员威胁和外部威胁，让人员能以更具安保意识的方式来思考和行动，并得以识别和报告引起关注的行为或活动。这从而促使所有人员感到他们在安保制度中发挥关键作用，整体安保得到改善 — 不仅仅是航空安保，还包括更广泛的边境安保，而且不需要大量投资。从安检员到清洁工，从出租车司机到机场零售店工作人员，都可对改进航空安保做出重要贡献。

3.2 强有力和有效的安保制度必须积极主动，并由有能力的人员提供支持。此外，安保文化要取得成功，就必须在遵从既定程序、遵守强制规章、并在出现不可预见的情况时采取主动行动等方面，让人问责并给予激励。有效的安保管理体系(SeMS)可以提供实现这一目标的办法，通过提供有条理的系统性方法来管理安保，将安保管理和风险所有权深植于组织及其人员的日常活动中。

3.3 培训工作组建议鼓励所有国家、组织和实体接受并促进积极的安保文化，以便更快地交付全球航空安保计划优先成果 2 项下的适用行动。应该鼓励所有人通过投资人力资本、建立积极胜任的工作队伍，以确保培养贯穿整体系统的能力和力量。这将有助于实现人人皆知在安保制度中自身角色和责任的安保文化。此类行动可包括附录 A — 即航空安保专家组于 2018 年批准的安保文化工具包中强调的内容，其中包括但不限于：关于安保文化的初训和复训以及持续学习活动、高级领导促进安保文化、有针对性的沟通计划和持续的安保意识活动、并建立一个保证对举报人保密的报告制度。

3.4 培训工作组承认，要实现安保文化行为和意识的转型并将其从上到下深植于整个组织并不容易。为了获得最大效益，各国应采取多机构方式，让安保文化的支持不仅侧重航空安保，而且放眼于总体安保。培训工作组鼓励各国、各组织和业界立即采取实际步骤，开始进行鲜明高调的行为改变运动和其他实际行动，以促进其组织内强大和可持续的安保文化。

4. 高级别会议的行动

4.1 请航空安保高级别会议：

a) 认识到国际民航组织培训工作组和航空安保专家组迄今为促进积极的安保文化所做的工作；和

b) 鼓励各国、各组织和业界使用培训工作组安保文化材料，通过采取实际步骤加强各自管辖范围或组织内的安保文化，立即实现安保改进和长期变革。

— — — — — — — —

APPENDIX A

SECURITY CULTURE TOOLKIT

A priority action of the Global Aviation Security Plan (GASeP), as adopted by the Council of ICAO 10 November 2017, is to **Develop Security Culture and Human Capability**. This document produced by the ICAO Working Group on Training and endorsed by the ICAO Aviation Security Panel 19-23 March 2018 seeks to build and promote positive security culture by providing States and Industry with a toolkit of best practices.

Introduction

– What is Security Culture?

Security culture is a set of norms, beliefs, values, attitudes and assumptions that are inherent in the daily operation of an organisation and are reflected by the actions and behaviours of all entities and personnel within the organisation. Security should be everyone's responsibility - from the ground up. Effective security culture is about:

- Recognising that effective security is critical to business success;
- Establishing an appreciation of positive security practices among employees;
- Aligning security to core business goals; and
- Articulating security as a core value rather than as an obligation or a burdensome expense.

Benefits

The benefits of an effective security culture include:

- Employees (staff) are engaged with, and take responsibility for, security issues;
- Levels of compliance with protective security measures increase;
- The risk of security incidents and breaches is reduced by employees thinking and acting in more security conscious ways;

- Employees are more likely to identify and report behaviours/activities of concern;
- Employees feel a greater sense of security; and
- Security is improved without the need for large expenditure.

Tools for the implementation of a positive security culture

This toolkit is designed to assist organisations operating in the aviation industry in enhancing their security culture. It outlines a number of tools to support trainers and managers with embedding and sustaining strong security behaviours within the workforce. The tools are grouped under the following intervention areas:

POSITIVE WORK ENVIRONMENT	
DESIRED OUTCOME	TOOLS
A work environment which drives and facilitates a positive security culture.	**Clear and consistent: policy, processes, systems and procedures** – enshrine security in all corporate policy and procedures, including those areas which do not have a primary security focus, such as the organisation's management plan. Document clearly in writing: policy, processes, systems and procedures which support a positive security culture. Ensure the information is easy to understand, simple to follow, and readily accessible to staff who may want to refresh their understanding.
	Equipment, space, resources – provide staff with the resources they need to achieve a strong security performance. This may be in the form of additional screening equipment, or by providing extra staff at a security checkpoint, or the provision of appropriate IT equipment or machinery.
	Prompts – help employees to implement good security by reminding them what actions they need to take. This could be notices on doorways reminding them not to allow tailgating (drive too closely behind another vehicle); or a pop-up prompt when logging on/off a computer.
	Suggestions box – allow staff the opportunity to suggest ways in which security could be improved. Reward suggestions which result in changes and improvements.
	Targeted communications plan - invite experts or celebrities from outside of the organisation to endorse security practices through fun messages. This could be via a video or an article or an in-person presentation.
Staff who know what security behaviours are expected of them and who confidently and willingly demonstrate the behaviours.	**Performance appraisals –** document for every employee what security behaviours are expected of them and assess their performance against these behaviours as part of the appraisal process. Provide feedback on their security behaviours, recognition for positive security behaviour, and consequences or sanctions for failure to adhere to security policy.
	Thank you messages - this may be in the form of a blog or an article on how strong security culture is impacting positively on the organisation. Or a corporate communication on the results of security checks e.g. 100% of employees were clearly displaying their security pass.
An organised, systematic approach to managing security which embeds security management into the day-to-day activities of the organisation and its people.	**Security Management System (SeMS) –** manage security in a structured way by implementing a SeMS. A SeMS can provide a risk-driven framework for integrating security into an organisation's daily operations and culture. The philosophy of SeMS is a top-to-bottom culture that leads to the efficient provision of a secure operation.

TRAINING	
DESIRED OUTCOME	TOOLS
Staff who have the knowledge, skills and capability to practice good security.	**Induction training** – equip employees with the knowledge, skills and abilities to practice good security from the outset. This includes those whose roles do not involve the implementation of aviation security measures. Educate new staff on the threat, in particular those who may pose a threat to civil aviation and their possible motives; the types of attack on aviation; and the reasons why aviation is an attractive target. Emphasise the importance of challenging non-compliance with security procedures/policy and include details of how to respond to security incidents. Provide examples of unusual/suspicious behaviour/items which should be reported. Use case studies, dummy items and role play to emphasise the message.
	Refresher training – provide refresher training at regular intervals so that employees can renew and update their knowledge of security matters. Training should include updates on emerging threats/recent incidents, security failures, suspicious behaviours and what to watch out for.
	Continuous learning activities – promote security messages throughout the year and support employees in expanding their security knowledge and skills. This may be in the form of security events, support with e-learning, and job shadowing or mentoring.
LEADERSHIP	
DESIRED OUTCOME	TOOLS
An environment where managers and leaders, including those at the highest level, lead by example and support their staff in implementing good security.	**Leadership briefings** - promote security messages through senior staff. Senior leaders could include security in part of their newsletters or staff briefings, or write an article or a blog on underlining the importance they place on good security and the actions they take personally to enhance and promote positive security culture.
	Example behaviour – support and personally apply security policy at all times and do not cut corners e.g. to save time.
	Patience and understanding - allow all staff the necessary time and resources to comply with security measures, even when under pressure.
	Thank you messages – personally thank those who have reported suspicious activity or security breaches.
	Involvement in security awareness events and staff briefings – senior management taking time to get personally involved in security awareness briefings and events. This would send a message to staff that managers/leaders have placed importance in security and are supportive for ongoing security initiatives.

UNDERSTANDING THE THREAT	
DESIRED OUTCOME	TOOLS
	Targeted threat briefings – provide middle and senior managers with targeted, more detailed threat briefings to maintain and enhance their understanding and appreciation of the threat.
All staff understand the nature of the threats they and their organisation face.	**Reminder briefings** – deliver regular reminders to existing staff and the wider airport community on security threats faced by the organisation. This could be via the intranet, in newsletters, at staff meetings, through annual refresher training or at specific coordinated briefing awareness sessions.
	Verbal updates when the threat picture changes – inform staff as soon as possible about new and emerging threats, or changes in threat level, and the implications of this for them and the organisation. This is best done face-to-face e.g. at staff meetings and shift briefings to allow staff to ask questions.
VIGILANCE	
DESIRED OUTCOME	TOOLS
All staff feel able to challenge those who are not complying with security policy /procedures.	**Repetition** – repeat messages for consistency and to help embed awareness. For example a person getting the same security messaging on recruitment, during induction, on pass issue, and throughout their employment.
	Reminder briefs - encourage staff to challenge non-compliance via briefings, handouts and posters in staff rest areas pointing out potential consequences of failing to challenge.
All staff and visitors pay attention to their surroundings when at the airport and know what unusual or suspicious behaviour looks like.	**Visitor briefing note -** create a short security briefing note to issue to all visitors along with visitors pass. The note could highlight the importance of paying attention to their surroundings when at the airport and provide contact details for the security room.
	Posters and signage – place signage around airport premises to remind staff and visitors to remain vigilant and pay attention to their surroundings. Contact details can be provided on the signage to advise the person who to contact if they detect suspicious personnel or activities.
	Regular security awareness campaigns – run security education campaigns at regular intervals to remind existing employees and airport operators about their role in protective security, what may constitute suspicious activity and the importance of reporting unusual behaviour or items. The campaign could include posters listing suspicious activities in staff rest areas, a blog or article on the intranet, including real-world examples or experiences, and a security awareness event showcasing protective security

	arrangements, with expert speakers, displays and presentations.
REPORTING SYSTEMS	
DESIRED OUTCOME	TOOLS
Security breaches and occurrences are reported swiftly and corrected. Staff do not feel as though they are 'telling tales' when reporting an incident.	**A just culture reporting system -** establish a reporting system that guarantees confidentiality of reporting individuals (a "just culture" reporting system) and include information on how to report breaches/occurrences via posters in staff rest areas.
	Induction training on reporting of security breaches - deliver training on the functioning of the "just culture" reporting system, its benefits and employees rights, responsibilities and duties in relation to occurrences as part every staff member's induction
	Rewards/Thank you - reward staff members who report security breaches and occurrences e.g. personal thank you from senior leaders, or recognition within the performance management system so that they know their report has been received and taken seriously.
INCIDENT RESPONSE	
DESIRED OUTCOME	TOOLS
All staff know how to respond and who to contact in the event of an incident.	**Wallet card** - issue to all employees a wallet-sized quick reference card containing details of who to contact for each type of security incident e.g. the number for reporting unusual or suspicious behaviour, reporting a lost company item etc. Cards could be made to fit into/to the back of airport/crew pass holders so to be always on hand.
	Regular table top exercises and practice drills – provide staff with the opportunity to think through the actions they may take during an incident and test their ability to respond to a situation. Lessons should be identified and recorded with changes in plans and procedures implemented where necessary.
INFORMATION SECURITY	
DESIRED OUTCOME	TOOLS
Sensitive information is stored, transmitted and disposed of securely and is shared only with those who need to know.	**Induction training** - deliver training on protecting and sharing information securely to all new employees with a test or other assessment to confirm understanding.
	Clearly documented information security policy and procedures – ensure this is readily accessible to staff who may want to refresh their understanding.
	Cyber Security - have robust cyber incident response plans in place. These plans should be tested and updated on a regular basis, with mechanisms in place to implement lessons learned

	from exercises and real life incidents.
	Reminder briefs - use briefings, handouts and posters in staff rest areas to remind staff of the importance of good information security, pointing out potential consequences of an information breach.
Lost/stolen items such as laptops, phones or papers are reported immediately.	**Wallet card/quick reference intranet page –** containing an easy to follow information on actions to take when company items have been lost or stolen.
MEASURES OF EFFECTIVENESS	
DESIRED OUTCOME	TOOLS
Improvements in security culture are being made.	**Breach records** - record the number of security incidents reported and allow an element of analysis to improve areas of weakness.
	Inspection results – record compliance rates with security policy e.g. number of staff correctly displaying their pass during inspections.
	Staff surveys/focus groups – carry out surveys to find out how staff feel about security and the culture.

— END —