TOOLKIT ON ENHANCING SECURITY CULTURE

A priority action of the Global Aviation Security Plan (GASeP), as adopted by the ICAO Council on 10 November 2017, is to develop security culture and human capability. This document, created by the Aviation Security Panel's Working Group on Training, 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 organization and are reflected by the actions and behaviours of all entities and personnel within the organization. Security should be everyone's responsibility - from the ground up. Effective security culture is about:

- Recognizing 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 burdensome expense.

Benefits

The benefits of an effective security culture include:

- Employees 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.

ICAO

November 2018

Tools for the implementation of a positive security culture

This toolkit is designed to assist organizations operating in the aviation industry in enhancing their security culture. It outlines a number of tools to help trainers and managers embed and sustain 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 and document clearly in writing. Ensure the information is easy to understand, simple to follow, and readily accessible to staff who may want to refresh their understanding.
	Equipment, space and 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 or signage; 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 organization to endorse security practices through messages.
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 organization. Or a corporate communication on the results of security checks e.g. 100 per cent of employees were clearly displaying their security pass.
An organized, systematic approach to managing security which embeds security management into the day-to-day activities of the organization 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 organization'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 all employees with the knowledge, skills and abilities to practice good security from the outset, including knowledge about the threats to aviation security. Emphasize the importance of challenging non-compliance with security procedures/policy and how to respond to security incidents. Provide examples of unusual/suspicious behaviour/items which should be reported.
	Refresher training – provide refresher training at regular intervals so employees can renew their knowledge of security matters to include new threats, security failures and suspicious behaviours.
	Continuous learning activities – promote security messages throughout the year and support employees in expanding their security knowledge and skills.

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 their newsletters or staff briefings, or write an article or a blog to underline the importance they place on good security and the actions they take personally to enhance and promote a 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
All staff understand the nature of the threats they and their organization face.	Targeted threat briefs – provide middle and senior managers with targeted, more detailed threat briefings to maintain and enhance their understanding and appreciation of the threat.
	Reminder briefs – deliver regular reminders to existing staff and the wider airport community on security threats faced by the organization. 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 organization.

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.
	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 their visitor's pass. The note could highlight the importance of paying attention to their surroundings when at the airport and provide contact details for the security control 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 staff and visitors who to contact if they detect suspicious persons 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 examples or experiences, and a security awareness event showcasing protective security arrangements.

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.
	Induction training on reporting of security breaches - deliver training on the functioning of the "just culture" reporting system to all employees, to include roles and responsibilities.
	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.

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.
	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 policy and procedures on information security – 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 analysis for improvement.
	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 culture.