SOUTH AFRICAN CIVIL AVIATION AUTHORITY

TECHNICAL GUIDANCE MATERIAL for Security Culture

SUBJECT: TECHNICAL GUIDANCE MATERIAL FOR ENTITIES TO PROMOTE, DEVELOP AND IMPLEMENT SECURITY CULTURE.

EFFECTIVE DATE: 29 MARCH 2022

APPLICABILITY

This guidance material is applicable to entities such as: Airports, Airlines, Ground Handling Service Providers, Regulated Agents, Known Consignors, Air Navigation Service Providers, Catering Stores and Catering Supplies Service Providers, Aviation Security Training Organizations, Aviation Security Screening Organizations and any aviation participant designated by the Minister in terms of Section 111 (1) (d) of the Aviation Act.

PURPOSE

The purpose of this guidance material is to provide guidance to relevant aviation entities to promote, develop and implement security culture.

REQUIREMENTS

Effective security implementation and establishing an appreciation of positive security practices in the organisation to Align security with core business goals

1. REFERENCE

i. ICAO Annex 17
ii. ICAO Doc 8973, Aviation Security Manual
iii. Civil Aviation Regulations, 2011
iv. ICAO Toolkit on Enhancing Security Culture

2. LIST OF ABBREVIATIONS

ABBREVIATION	DESCRIPTION
AVSEC	Aviation Security
E	Executive
E: AVSEC	Executive: Aviation Security
NASP	National Aviation Security Programme
SACAA	South African Civil Aviation Authority

SACARs	South African Civil Aviation Regulations
SACATS	South African Civil Aviation Technical Standards
SM	Senior Manager
SM: DC	Senior Manager: Dangerous Goods and Cargo Security

3. SECURITY CULTURE

3.1. General

3.1.1. Security culture is an organizational culture that encourages optimal security performance. Organizational culture is generally understood to be a set of norms, beliefs, values, attitudes and assumptions that are inherent in the daily operation of organizations and are reflected by the actions and behaviours of all entities and personnel within those organizations. Security culture cannot be considered in isolation from the organizational culture as a whole.

3.1.2. In order to establish or improve security culture in organizations, measures could be developed to enhance such norms, beliefs, values, attitudes and assumptions. Those enhancements should aim at furthering the following principles:

a. continuously improve security, encompassing the effectiveness and efficiency of security in mitigating security risks.
b. encourage awareness of and alertness to security risks by all personnel and the role that they personally play in identifying, eliminating or reducing those risks.
c. encourage familiarity with security matters, procedures and response mechanisms (e.g., whom to call in case of suspicious activity).
d. allow the necessary time and make the necessary efforts to comply with security measures, even when under pressure.
e. promote willingness to accept responsibility, be pro-active and make decisions autonomously in the event of security occurrences (which include incidents, deficiencies and breaches).
f. challenge other personnel in case of irregularities and accept being challenged.
g. immediately report incidents or any suspicious activity that might be security related.
h. foster critical thinking regarding security and interest in identifying potential security vulnerabilities,
i. handle sensitive aviation security information appropriately.

3.2. Applicability, objectives, and benefits

3.2.1. Entities such as Airports, Airlines, Ground Handling Service Providers, Regulated Agents, Known Consignors, Air Transport Service Providers, Catering Stores and Catering Supplies Service Providers, Aviation Security Training Organizations, Aviation Security Screening Organizations and any aviation participant designated by the Minister in terms of Section 111 (1) (d) of the Aviation Act., security service providers and any other entity potentially playing a role in the safeguarding of civil aviation against acts of unlawful interference, including entities whose activities are not primarily security-focused, should develop and assess measures and mechanisms that may contribute to establishing security culture as an essential aspect of aviation security.

3.2.2. The establishment of a security culture should assist organizations in improving their overall security performance through the early identification of potential security challenges. Organizations should also develop methods of measuring the effectiveness of the security culture, which would allow them to evaluate its effect on security and the changes that occur over time.

3.2.3. Benefits to implementing a security culture amongst others include:

a. Employees are more engaged with security matters and take responsibility for security.
b. Overall compliance with security measures increases.

c. The risk of security incidents and breaches is reduced by employees thinking and acting in a more security conscious ways;
d. Employees are more likely to identify and report suspicious behaviours/activities.
e. Employees feel a greater sense of security; and
f. Security is improved without the need for additional expenditure.

3.3. Leadership in security culture

3.3.1. Just as leaders have a critical impact on organizations and their culture, organizational cultures greatly influence leaders by guiding their decisions. Organizations should therefore ensure that the full commitment at every level of leadership, from top management to supervisors, is applied at all times and in all activities, strategies, policies and objectives in order to continuously improve the security culture.

3.3.2. Management should lead by example and encourage all personnel (including contractors and third-party service providers authorized to act on behalf of the organization) to adopt a security mindset by advocating security as an organizational and personal value and aligning their own behaviour with this value. For instance, aviation managers and executives could:

a. abide by rules always set out in aviation security and lead by example.
b. continuously promote and support the importance of security measures.
c. regularly engage in dialogues regarding security issues with peers and personnel.
d. encourage and be receptive to constructive feedback regarding security occurrences.
e. process security occurrences and reports in a timely fashion and implement any required corrective and preventive actions as necessary.
f. intervene appropriately whenever security is compromised notwithstanding potential economic consequences; and
g. support training and capacity-building for security needs.

3.3.3. Security should become an underlying value of the organization, reflected in its management strategies, policies and objectives. Every entity playing a role in aviation security, including those whose activities are not primarily security-focused, could therefore:

a. define the optimization of security as one of the basic goals of the organization.
b. enshrine aviation security in the written policies of the organization, constituting an integral part of the company’s management plan; and
c. consider security in all processes of the organization’s work.
d. Promote a “Just culture” reporting systems

3.3.4. Just culture systems refer to reporting systems through which occurrences can be reported anonymously or confidentially to an independent entity, thereby allowing reporting individuals to be exempted from any kind of retaliation under specific circumstances. Such systems aim to encourage individuals to report occurrences that would otherwise remain unnoticed and would therefore not be corrected.

3.3.5. Entities should consider the introduction of a “just culture” reporting system for security occurrences, drawing from the experience gained from the establishment and implementation of just culture systems in safety.

3.3.6. Exemptions from punishment may be granted only in cases where the legal basis allows for such exemptions and where reporting individuals have not acted wrongfully on purpose or in culpable negligence. In case of severe security occurrences, which include incidents, deficiencies and breaches, exemption from punishment should not normally be granted to perpetrators, even if they willingly reported the occurrence.

3.3.7. Security occurrences do not necessarily result in harm to persons or damage to property. Indeed, security occurrences need to be coupled with the intentional or unlawful act of an individual in order to potentially result in harmful consequences. Experiences gained from implementing aviation safety reporting programmes can be of great value in developing similar programmes for aviation security.

3.3.8. Aviation organizations and other entities playing a role in aviation security could implement a just culture reporting system by:

a. establishing a system that guarantees confidentiality of reporting individuals whereby personal data is not collected and/or stored. Where personal data is collected it should be used only to either gain clarification and further information about the reported occurrence, or to offer feedback to the reporter.
b. identifying an independent body or person tasked with managing, maintaining and guaranteeing the confidentiality of data collections, as well as analysing and following up on reports.

c. providing appropriate training on the functioning of the just culture reporting system, its benefits, and individuals' rights, responsibilities and duties in relation to occurrences; and
d. implementing an incentive programme aimed at encouraging personnel to report occurrences, while preventing malicious and defamatory reporting. Such a programme should also encourage personnel to provide constructive feedback on security measures with a view to improving the system as a whole and achieving greater security performance.

3.3.9. A clear, single point of contact to coordinate reporting should be established within the organization in order to facilitate the process for personnel as much as possible. Many entities already have systems for safety reports in place and could simply extend them to accommodate security reports.

3.4. Leadership Tool

DESIRED OUTCOME	ACTION STEPS
Establish an environment where managers and leaders, including those at the highest level, led 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/leader have placed importance in security and are supportive for ongoing security initiatives.

3.5. Reporting Systems Tool

DESIRED OUTCOME	ACTION STEPS
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.

3.6. Quality control

3.6.1. Organizations could implement quality control programmes designed to monitor the effective implementation of security measures. Quality control programmes can be an effective tool in keeping personnel alert and committed to security culture principles. The frequency and rigidity with which quality controls are carried out may have a positive influence on personnel by demonstrating management’s commitment to security objectives and compliance.

3.6.2. Regular quality controls of the reporting mechanisms in place should be carried out as part of the quality control programmes. Security culture measures applied by appropriate authorities.

3.6.3. Appropriate authorities should lead by example and commit to strengthening their internal security culture just as they should engage in strengthening the security culture of the entities implementing aviation security measures.

3.6.4. Awareness training, awareness campaigns and related measures may be efficient mechanisms to ensure a continuous and appropriate commitment to security norms, beliefs, values, attitudes, and assumptions. They may also increase knowledge of do’s and don’ts with regard to sharing, storing and protecting sensitive security information.

3.7. Coordination among entities

3.7.1. Entities playing a role in aviation security should establish an internal security committee which will meet on a regular basis to assess the security performance of their organizations and identify priorities and specific measures to improve performance, including measures to promote security culture.

3.7.2. The committee should be composed of senior leaders in addition to security managers and should coordinate projects led by specialized groups within the organizations.

3.7.3. In the case of airports, a joint stakeholder security committee with other entities such as aircraft operators and security service providers, should be established.

3.7.4. The aim of this committee is to identify areas of improvement with a goal of achieving greater security performance. For example, the committee may jointly decide on the conduct and content of security awareness campaigns or agree on the promotion of mutually reinforcing measures.

3.8. Internal communication

3.8.1. Senior management should ensure that legal obligations and internal guidelines regarding security, as well as the reason for their introduction, are duly communicated to all personnel.

3.8.2. A robust internal communication programme contributes to the acceptance and understanding of security measures by all personnel and helps promote the norms, beliefs, values, attitudes and assumptions of the organization.

3.8.3. In addition, internal communication programmes may greatly assist management in:

a. ensuring that all personnel are fully aware of their duties and rights, as well as the reporting mechanisms in place in the organization and vis-à-vis the appropriate authority; and
b. promoting a code of practice regarding security, consisting of simple principles guiding staff conduct in their everyday work and during crisis situations.

3.9. Awareness training

3.9.1. All personnel of state entities operating within the aviation environment and entities involved in civil aviation (regardless of roles or functions) should undergo security awareness training where it is not already part of specific role or functional training to ensure that they are adequately knowledgeable in aviation security measures, security objectives and related matters. Such training may be informational or educational, as appropriate. It could also be adapted to the audience, as practicable, and inform on changes in security measures, objectives and related matters.

3.9.2. Security awareness training should be delivered to all personnel upon their hiring and may include the following subjects:

a. purpose of awareness training.
b. briefings on threats and risks to civil aviation and potential consequences in case of insufficient safeguarding or complacency.
c. identification of the role that the organization plays in safeguarding against acts of unlawful interference; recognition of what may be considered as suspicious activities.
d. identification of the role of all players in improving the security culture of their organization.
e. recommendations for the introduction of measures that may help improve the security culture in the organization.
f. briefings on communication mechanisms.
g. procedures for occurrence-reporting mechanisms (i.e. just culture reporting system) and follow-ups; and
h. proper handling of sensitive aviation security information.

3.9.3. Organizations should consider conducting workshops to help personnel better understand each other's functions and assist managers and supervisors in collecting valuable feedback and experiences from personnel. Real-life scenarios, tabletop exercises and/or drills should also be considered as a way to simulate incidents and better understand their associated response mechanisms.

3.9.4. Organizations should clearly define the requirements and content of their awareness training in the approved security programmes.

3.10. Awareness Training Tool

DESIRED OUTCOME	ACTION STEPS
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.

3.11. Security awareness campaign

3.11.1. Security awareness campaigns may be an efficient mechanism to ensure a continuous and appropriate commitment to security norms, beliefs, values, attitudes and assumptions.

3.11.2. Such campaigns, when conducted frequently, may also assist management in ensuring that all personnel remain alert, do not become complacent, and continue to adhere to their organization's security culture.

3.11.3. Security awareness campaigns may be in the form of:

a. flyers and posters highlighting the importance of specific security measures. Management should solicit the assistance of personnel in disseminating flyers and posters to the rest of the organization to demonstrate a common commitment to security measures. These publications should not provide any details of security measures in place if the general public may have access.
b. walk-in exhibitions and workshops gathering all types of personnel, including management, to help better understand the importance of security in the organization and the reasons for the measures in place;
c. regular briefings, which allow for continuous awareness of security measures.
d. e-learning tools; and
e. internal communication platforms such as intranet, newsletters, brochures, and videos.

3.12. Vigilance Tool

DESIRED OUTCOME	ACTION STEPS
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.
	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.

3.13. Positive work environment

3.13.1. A positive work environment may also greatly influence the commitment of personnel to the security culture of their organization and enhance security performance.

3.13.2. A positive work environment should include, at a minimum:

a. the involvement of personnel in decision-making processes (e.g., considerations of identified security gaps, suggestions for improvement to the security awareness training programme and other security policies and procedures);
b. the allocation of sufficient time for personnel to perform security tasks.
c. a mechanism for recognizing individual good performance (i.e., incentives and reward programme).
d. a reporting system encouraging staff to submit useful suggestions and observations.
e. the provision of feedback to personnel, in particular on reported suggestions and observations.
f. the setting of clear, achievable, and measurable goals.
g. the provision of the necessary tools (e.g., appropriate training and procedures) to enable personnel to achieve their goals; and
h. the provision of an adequate level of autonomy and responsibility to personnel.

3.13.3. Positive Work Environment Tool

DESIRED OUTCOME	ACTION STEPS
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.
	Suggestion's 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	Performance appraisals – document for every employee what security behaviours are expected of them and assess their

DESIRED OUTCOME	ACTION STEPS
willingly demonstrate the behaviours.	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-today 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.

3.14. Measuring the effectiveness of security culture

3.14.1. Organizations implementing measures to enhance their security culture (i.e., norms, beliefs, values, attitudes and assumptions) and improve their overall security performance should develop a performance indicator framework designed to qualitatively assess the impact on the security culture of measures in place as well as determine the gap existing between the desired and actual culture outcomes.

3.14.2. As some elements of security culture may not be directly observed, a range of possible indicators have been demonstrated as allowing organizations to effectively assess the strength of norms, beliefs, values, attitudes and assumptions. Measures for these indicators may be obtained from questionnaires or online surveys. Open interviews help to complement information about the security culture of an organization.

3.14.3. Quality assurance programmes should include tools designed to capture all relevant information regarding the effectiveness of security culture and measures in place.

Note: As per ICAO (2021) Information on performance indicator tools designed to measure the effectiveness of a security culture can be found on the internet. For example, the Centre for the Protection of National Infrastructure (www.cpni.gov.uk) has published a security culture survey and analysis tool called 'SeCuRE 3' to help organizations assess and understand their security culture.

3.15. Measures of Effectiveness Tool

DESIRED OUTCOME	ACTION STEPS
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.

3.16. Additional Tools for the implementation of a positive security culture

Below are additional tools that could be implemented to establish a security culture within an organisation:

3.17. Understanding The Threat Tool

DESIRED OUTCOME	ACTION STEPS
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.

3.18. Incident Response Tool

DESIRED OUTCOME	ACTION STEPS
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 tabletop 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.

3.19. Information Security Tool

DESIRED OUTCOME	ACTION STEPS
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	Wallet card/quick reference intranet page – containing an

reported immediately	easy-to-follow information on actions to take when company items have been lost or stolen.

DEVELOPED BY:		
	NICO SMIT	29 MARCH 2022
SIGNATURE OF SM: DC	NAME IN BLOCK LETTERS	DATE
APPROVED BY:		
	LUVUYO GQEKE	29 MARCH 2022
SIGNATURE OF E: AVSEC	NAME IN BLOCK LETTERS	DATE

END