ICAO Security Culture Guidance Material

What is security culture?

1. Security culture is an organizational culture that encourages optimal security performance. Security culture is commonly 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.

2. Effective security culture is about:

    a) recognizing that effective security is critical to business success;

    b) establishing an appreciation of positive security practices among employees;

    c) aligning security to core business goals; and

    d) articulating security as a core value rather than as an obligation or burdensome expense.

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

    a) continuously improve security, recognizing that a security culture in an organization is an essential component of an effective, proactive and reactive security regime, which supports and maintains a risk-resilient structure that helps to manage effectively both insider and external risks;

    b) encouraging 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) encouraging familiarity with security issues, procedures and response mechanisms (e.g. whom to call or processes to report in case of suspicious activity);

    d) recognizing the importance of security from all levels of an organization, including management, and reflecting that through the observation and participation in all security measures;

    e) allowing the necessary time and making the necessary efforts to comply with security measures, even when under pressure;

    f) promoting willingness to accept responsibility, to be pro-active and to make decisions autonomously in the event of security occurrences, which include incidents, deficiencies and breaches;

    g) challenging other personnel in case of irregularities and accept being challenged (i.e., promote speaking up, acknowledge different perceptions);

    h) immediately reporting occurrences or any suspicious activity that might be security-related – independent of who is doing it;

    i) fostering critical thinking regarding aviation security and interest in identifying potential security vulnerabilities, deviation from applicable procedures, and solutions; and

    j) handling sensitive aviation security information appropriately.

Applicability, objectives and benefits

4. Entities involved with or responsible for the implementation of the National Civil Aviation Security Programme (NCASP), such as appropriate authorities, security service providers and any other entity potentially playing a role in the safeguarding of civil aviation against acts of unlawful interference, should promote, develop and implement measures and mechanisms that may contribute to establishing security culture as an essential aspect of aviation security, while also assessing whether the measures implemented are working properly. This should include entities whose activities are not primarily security-focused as security should be everyone's responsibility.

5. The establishment of an effective security culture should assist organizations in improving their overall security performance through the early identification of potential security challenges. Organizations should develop a robust security culture policy that is supported by leadership and which aims to promote and implement a positive security work environment; reporting and incident response systems; initial and recurrent security training, to include training on security awareness, threats to aviation, and security roles and responsibilities; security awareness campaigns; vigilance and information security.

6. The benefits of an effective security culture includes:

    a) employees are engaged with, and take responsibility for, security issues;

    b) levels of compliance with protective security measures increase;

    c) the risk of security incidents and breaches is reduced by employees thinking and acting in more security-conscious ways;

    d) employees are more likely to identify and report behaviours/activities of concern;

    e) employees feel a greater sense of security; and

    f) security is improved without the need for large expenditure.

Note 1. — For those States or entities that choose to adopt a Security Management System (SeMS) approach, the promotion of a strong security culture which embeds security management into the day-to-day activities of an organization is an essential component.

Note 2. — A Security Culture Toolkit, developed by ICAO, can be found on the ***ICAO Security Culture website***[1]*. It provides an array of tools designed to help States and industry build and promote an effective security culture.*

Leadership in security culture

7. 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.

8. 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

[1] www.icao.int/Security/Security-Culture/Pages/ICAO-Resources.aspx

security as an organizational and personal value, and aligning their own behaviour with this value. For instance, aviation managers and executives should:

a) abide by security rules at all times 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.

9. 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, should 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.

"Just culture" reporting systems

10. Just culture systems refer to reporting systems through which suspicious 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.

11. Appropriate authorities 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, and following the same principles.

12. When a person reports a security event or a security concern, a just culture reporting system requires that all reported occurrences be taken seriously and investigated on a systemic level, using incident cause analysis models of investigation, not on the level of any human inevitable performance variability.

13. Punishment should be applied only in cases where the legal basis provides for such penalties. Exemptions should be guaranteed for situations where the individuals who reported have not acted wrongfully on purpose or in culpable negligence. In the case of serious security occurrences, which include incidents, deficiencies and violations, the exemption from punishment should not normally be granted to perpetrators, even if they voluntarily report the occurrence. Organizations must make explicit where the limits are between acceptable and unacceptable behaviour and seek agreement on the consequences if these limits are exceeded.

14. 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.

15. Appropriate authorities, organizations and other entities playing a role in aviation security should 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 anonymous and 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.

16. 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.

Quality control

17. Organizations should 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 effective 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.

18. 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

19. 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. They should support their staff by:

    a) leading by example, abiding by the aviation security rules at all times; and

    a) promoting and supporting the importance of the security measures.

20. Through leadership briefings, support messages and involvement in security-related events, appropriate authorities can advertise effective security to staff and ensure a continuous and appropriate commitment to security norms, beliefs, values, attitudes and assumptions. Through those mechanisms, the knowledge of "do's and don'ts" with regard to sharing, storing and protecting sensitive security information may also increase.

Security culture measures applied by entities playing a role in aviation security

Coordination among entities

21. 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 an effective security culture. The committee should be composed of senior leaders in addition to aviation security managers and should coordinate projects led by specialized groups within the organizations. This group should contain stakeholders outside aviation security entity, such as representatives from an organization's communications, marketing, and human resources departments.

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

Internal communication

23. 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. A robust internal communication programme contributes to the acceptance and understanding of security measures by all personnel. It should be simple to follow and readily accessible, and help to promote the norms, beliefs, values, attitudes and assumptions of the organization.

24. 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.

Awareness training

25. All security and non-security staff and personnel working at the airport should undergo security awareness training where it is not already part of a specific role or function training, on both an initial and recurring basis. This is to ensure that they are 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.

26. Security awareness training should be delivered to all personnel upon their hiring or before being allowed unescorted access to security restricted areas of airports or to secure cargo, inflight supplies or airport supplies areas. Such security awareness training may include the following subjects:

    a) purpose of training on security awareness;

    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;

d) recognition of what may be considered as suspicious activities;

e) identification of the role of all players in improving the security culture of their organization;

f) recommendations for measures that may help improve the security culture in the organization;

g) briefings on communication mechanisms;

h) procedures for occurrence-reporting mechanisms (i.e. just culture reporting system) and follow-ups; and

i) proper handling of sensitive aviation security information.

27. 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.

28. Organizations should clearly define the requirements and content of their security awareness training (in the case of an appropriate authority, it should be defined in the National Civil Aviation Security Training Programme). The use of e-learning tools may be an appropriate method of delivering security awareness training. The content of a security awareness course should be adapted to the profile of the personnel to be trained.

Security culture campaigns

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

30. Security culture campaigns may be in the form of:

a) flyers and posters highlighting the importance of specific security measures or targeted messages. 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) face-to-face meetings such as regular briefings, airport pass collection, and training, which allow for continuous awareness of security measures;

d) announcements, including public announcements;

e) e-learning tools; and

f) internal communication platforms such as intranet, newsletters, brochures and videos.

Note — A Security Culture Campaign Starter Pack, developed by ICAO, can be found on the ***ICAO Security Culture website***[2]***.*** *This starter pack is designed to help everyone in the aviation sector raise the profile of security and to encourage all staff, including service providers and members of the wider aviation community, to think and act in a security-conscious manner.*

Positive work environment

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

    a) influencing employees' commitment to their organization's security culture and striving to maintain or enhance security performance;

    b) a work environment that facilitates an effective security culture;

    c) staff who understand and demonstrate security behaviours; and

    d) an organized, systematic approach to managing security.

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

    a) the involvement of personnel in the risk assessment process, to include analysis and, understanding of the results, as well as in the 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.

Measuring the effectiveness of security culture

33. Organizations (including appropriate authorities) should develop an action plan which will define the measures to be implemented with a view to obtaining the desired security culture outcomes. The action plan should contain details of the measures to be implemented and should be part of security culture policy. Targets, deadlines and milestones should be defined for each measure.

34. Organizations (including appropriate authorities) implementing measures to enhance their security culture and

[2] www.icao.int/Security/Security-Culture/Pages/ICAO-Resources.aspx

to improve their overall security performance should develop a key performance indicator framework. The framework should be designed to qualitatively and quantitatively assess the impact of measures in place on the security culture, as well as determine the gap existing between the desired and actual culture outcomes.

35. 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 key performance indicators may be obtained from quality control activities, such as inspections, breach records, reports of suspicious activity and occurrences, observational data or survey data and/or from qualitative tools, such as questionnaires, as well as open interviews. This will help to complement information about the security culture of an organization.

36. Examples of desired security culture outcomes, measures, key performance indicators and targets include:

Outcome	Measure	KPI	Target
An effective system for reporting incidents, security breaches, security incidents and suspicious behaviours.	Implement a just culture report system	Number of reports of the identification of security breaches, security incidents and suspicious behaviours.	Increase % of the number of reports of the identification of security breaches, security incidents and suspicious behaviours compared to the initial situation.
Personnel, including those who have unescorted access to the security restricted areas of the airports, with the capacity and ability to identify suspicious behaviours.	Awareness campaign	Number of reports of the identification suspicious behaviours.	Increase % of the number of reports of the identification suspicious behaviours compared to the initial situation.
A work environment that fosters, promotes and facilitates an effective security culture within the organization.	Clear / consistent definition and/or review of internal processes and procedures	Number of non-compliances related to unclear and/or inconsistent internal processes and procedures	Decrease % of the number of non-compliances related to unclear and/or inconsistent internal processes and procedures

37. Organizations should undertake an evaluation study to gauge where the organization was (in relation to the key performance indicators) prior to implementing measures to enhance their security culture and improve their overall security performance. After measures are implemented, the organizations should rerun the evaluation study on a recurring basis (e.g., once per year) to measure progress and to gather feedback on whether the approach was resonating and having the desired effect.

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

— END —