Information Sheet on Security Culture
Jointly Developed by Singapore and the United States of America

What?

Security culture refers to a set of security-related norms, 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.

Why?

Security culture can help organisations achieve the following:

a) As a core organisational value, enhance the security of the operation by enabling the engagement of a workforce that possesses a strong security mindset;
b) Support organisational goals by becoming an integral part of its operations as well as product offerings; and
c) Contribute to the resilience of operations and processes, particularly during high risk period.

Who?

Security is not merely the concern and responsibility of security agencies and organisations. Everyone, from members of the public and passengers to employees working at the airport, has a stake in maintaining the security of aircraft and the airport and civil aviation facilities.

Benefits of an effective security culture

An effective security culture can bring the following benefits to an organisation:

a) Contributes to reducing vulnerability by mitigating security risks;
b) Provides a sense of ownership to the staff by knowing that their actions create a safer flying experience;
c) Sets an environment that passengers can expect and rely upon when they travel;
d) Increases likelihood of staff reporting on suspicious behaviour and/or activities;
e) Enables swift and appropriate responses to security incidents;
f) Increases levels of compliance with security requirements;
g) Enhances security capabilities without the need for large expenditure; and
h) Facilitates a greater sense of security and responsibility amongst the workforce.

Elements of a Strong Security Culture

A strong security culture is imbued with the following elements:

a) A positive work environment that influences staff commitment to strive to enhance their organisation's security performance;
b) Staff equipped with necessary skills, knowledge and understanding on importance of security as well as proper procedure and processes to carry out the requisite tasks;
c) A clear understanding of the prevailing threats that the organisation is facing and how those threats change over time;
d) Explicit support from the organisation's management in promoting strong security culture. Management championing the importance of security, establish clear goals as well as setting the tone by being an example and provide support throughout the process;
e) A high level of vigilance amongst staff in looking out for suspicious behaviour and activities;
f) Effective reporting systems to enable giving fast attention to incidents and that possess clear reporting procedure and guidelines for staff to adhere to;
g) A clear incident response plan that not only specifies the roles and responsibilities of all staff in the organisation, but one which is also well-communicated;
h) A reward system that recognises and promotes positive security attitude displayed by staff;
i) Strong information security that secures sensitive security information and prevents misuse by unauthorised personnel; and
j) A system of constant review and monitoring, through measuring staff perceptions on security as well as their understanding of threat and risk, to determine the effectiveness of efforts in promoting strong security culture.

How?

Organisations looking to promote strong security culture may consider the following approaches:

a) Recruit and hire a capable and diverse team of exceptional individuals to start promoting security culture;
b) Establish effective communication channels and promote responsiveness, inclusion, and collaboration;
c) Retain, reward, and promote high performers and define career paths for advancement;
d) Develop and sustain the systems and infrastructure necessary to support our workforce; and
e) Foster an environment of continual learning and growth that instills shared organizational values and advances technical, critical thinking, and leadership skills:

    i. **Insider Risk Awareness Training:** Staff are provided with the definition of an insider threat, indicators, case examples, and reporting mechanisms;
    ii. **Security Awareness Training:** Provides an overview of how to identify suspicious activity, maintain situational awareness, and what staff need to know when reporting suspicious activity (e.g. "See something say something");
    iii. **Behavior Awareness Training:** Critical thinking, classroom-based training on establishing the environmental baseline and recognizing deviations, identifying suspicious behaviors, articulating suspicious behaviors, responding to behavioral threats, and reporting suspicious incidents; and
    iv. **Leadership Training:** Provides staff at all levels leadership fundamentals.

References

Various tools and resources are available to help to develop, maintain and sustain an effective security culture. You may refer to ICAO Toolkit on Enhancing Security Culture to learn more. The link is as follows: https://www.icao.int/Security/Security-Culture/Pages/ICAO-Resources.aspx