2021 | THE YEAR OF SECURITY CULTURE

ICAO

2021 THE ICAO YEAR OF SECURITY CULTURE (YOSC)

ENHANCING A POSITIVE SECURITY CULTURE WORKSHOP

Brief Introduction

- Air, Sea and Land transport operations are essential for social and economic development.
- Create opportunities for travel, trade and tourism
- Recent history has shown a genuine threat to Aviation sector from terrorist organizations seeking to disrupt operations.

Terrorist

- Cause significant economic and psychological impact
- Publicity – media
- Mass casualties

Criminals

- Criminals seek to exploit weaknesses in security to maintain their operations
- Drug importation
- People smuggling
- Money laundering
- Cyber security breaches

What is YOSC

- Year of Security Culture
- Aims to raise security awareness and promote a positive security culture in aviation operations worldwide
- Seeks to encourage and facilitate the enhancement of security behavior and practices
- Focus on the principle that Security is everyone's responsibility.

BACKGROUND INFORMATION

- The 40th Assembly designated 2020 as the Year of Security Culture (YOSC) making security awareness and security culture a priority
- The ICAO Council has approved a relaunch of the YOSC in 2021 due to COVID-19
- YOSC supports the GASeP priority action of “developing security culture and human capability”

Cont'd

- A Secretarial Project Team has been established to deliver and promote YOSC activities
- To ensure the YOSC is a success, global efforts are required
- Desire for a rolling worldwide programme of practical events to raise the profile of security in aviation.

Aims and Objectives

- To encourage the aviation industry to think and act in a security – conscious manner
- To embed security consciousness within normal airport operations – achieving a balance of security, safety, facilitation and passenger experience
- To promote an effective and sustainable security culture, as a critical core value endorsed from top management: "security is everyone's responsibility"

What is security culture?

- An organizational belief system that permeates all levels of an entity or company's management and staff – and which promotes awareness and individual responsibility for achieving security outcomes.

- "Set of norms, beliefs, attitudes and assumptions, that are shared by everyone that determine how people are expected to think about and approach SECURITY"

Effective security culture

- 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 a burdensome expense

Benefits of effective security culture

- Employees are engaged with, and take responsibility
- 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

Cont'd

- 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

Why is Security Culture Important?

Without a good security culture:

- Unintentional security breaches are likely to be more frequent
- It becomes harder to identify behaviours of concern
- Employees maybe more vulnerable to social engineering

- First impressions count, the organization may be perceived as an easy target

- Insider cases are often linked with a poor security culture.

- Insider threat

- External threat

Security Culture – Essential Components

Communication and Awareness of the threat

- Risks must be understood at all levels of the organization (e.g Airport Seniors)
- Staff undertake regular awareness training to develop awareness of risks
- Understanding risks helps to educate people as to why security is important to them and their organization.

Personal ownership/Senior Sponsorship

- All staff should take ownership and responsibility for their role in security
- Appropriate senior leaders and managers should visibly endorse security initiatives.

Clear Roles in Security

- Staff must understand clearly what their roles and responsibilities are in relation to security
- Clear guidelines and policies that are embedded in training
- Consistent application of security responsibilities that are properly enforced.

Incentives/Enforcement

- Deliberate or malicious security breaches must be dealt with consistently
- Careful consideration of how accidental security breaches are handled – a clear and consistent policy

Guidelines and Procedures

- Apply policies consistently
- Make policies accessible and available
- Consider channels for how the policies might be changed in response to feedback.

Reporting and Challenging

- Design reporting mechanisms that are easy to use and reinforce reporting behaviour
- Cultivate an atmosphere where it is acceptable to challenge people on their security.

Supportive Processes

- Security is sometimes seen as obstructive; design systems so that they work more effectively with other business needs
- Shape the environment to enable staff to enact security behaviours.

Factors inhibiting good security behaviours

- Can’t challenge someone senior who isn’t complying with security protocols
- Consequences – What if I get it wrong? Will I be in trouble?
- I don’t know who or how to report if I do see something
- Lack of time to think security – everyone is busy with their role.

Cont’d

- Lack of knowledge / communications
- Lack of education on current threat and training
- Those in non-security role – “ isn’t this why we have security / police personnel?”.

Interventions

- Senior commitment
- Continuous Improvement
- Commitment to adequate resources and training with clear responsibilities
- Communicate – Security is everyone's responsibility
- Clear security reporting procedures.

Big Foot and Avsec New Zealand Short videos as SUMMARY

- Use of Airport ID Pass
- Unattended Bag
- Access to Airside or Security Restricted Areas
- Recognizing suspicious behaviour
- Reporting