ICAO

GUIDE TO THE RUNNING OF A SECURITY CULTURE CAMPAIGN

SECURITY CULTURE CAMPAIGN - STARTER PACK

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.

There is advice and best practices on how to establish, change and maintain good security behaviours and information on delivering a security culture campaign.

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 and top-down. 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 a burdensome expense.

The pack is broken down into three sections:

Key Principles, Customizable Resources, and the **ICAO Toolkit for Enhancing Security Culture**.

icao.int

Part 1 - Key Principles

This section highlights key areas that all aviation personnel within an entity or organization should understand to prioritize security culture, and contains key principles on:

1. Obtaining Buy-in
2. Educating on the Security Threat
3. Enabling Staff
4. Retaining Buy-in
5. Communicating Methods
6. Creating an Implementation Plan
7. Evaluating Implementation
8. Responding to Suspicious Activity and Incidents

These principles can be used to motivate and facilitate culture change and to design a security culture programme

GUIDE TO THE RUNNING OF A SECURITY CULTURE CAMPAIGN

PART 1 - KEY PRINCIPLES

1. ### Obtaining Buy-in
   The key to your campaign being successful is a firm commitment from:
   - Management at all levels, including senior executives, who see security as an asset not a cost. Managers should:
     - Support security culture initiatives (being reassured that support will not negatively impact airport business);
     - Demonstrate that customers and passengers can be reassured by a strong security posture; and
     - Inform stakeholders that a robust security culture can increase customer satisfaction.
   - Key departments that can help, such as corporate communications, marketing and/or Human Resources, will understand the best ways of communicating with staff and suggest various lines of communication.

   Security culture develops because of the strategic direction agreed to by **senior management** and the associated behaviours it demonstrates and wants staff to follow. Embedding security culture into the management of the airport, i.e. beyond the immediate identification and resolution of suspicious activity, brings business continuity as well as broader benefits.

   Senior management should lead from the front and act as role models in delivering an effective security culture; for example, not being subject to exemptions from security measures or encouraging workarounds. Their behaviours are the best way to inspire staff to do the same.

2. ### Educating on the Security Threat
   All personnel need to be aware that the global aviation security threat is real and can manifest itself in many different risks. It is important for staff to understand that an incident could happen at any time, in any place and they – along with colleagues and the airport environment as a whole – could be the target or be impacted by the attack.

   It is important to ensure senior leaders and decision makers are educated on the threat to aviation. Without this awareness there will be a lack of desire to act and the campaign will be short lived, as other priorities will take precedence, resources will not be allocated to support implementation, and management will not know what their role should be in supporting this activity.

   Educating staff about threats and what the aviation sector has in place to counter them (including regulations and Standard Operating Procedures (SOPs)) helps allay concerns. Staff are less likely to adopt the required security culture behaviours when they are uninformed about the risks airports and airlines face and don't understand why security measures are in place.

   In addition, one of the indirect benefits of an effective security culture is a deterrence factor; reducing crime and other disruptive incidents while supporting the primary objective of maintaining a robust counterterrorism stance.

   Describe how this threat might play out in terms of targeting staff. Draw on **real-life examples** or incidents and attacks against aviation as they should resonate with staff better than hypothetical scenarios (the ICAO Risk Context Statement provides useful examples). These real-life examples will underscore how a threat may have operational, financial, and reputational consequences, affecting personnel safety and job security. This will help staff identify suspicious activity and be mindful of their own behaviour, as well as that of colleagues, and enhance vigilance.

3. ### Enabling Staff
   Staff can become complacent about risks and may believe that they have no contribution to make to security. If staff are not provided the necessary training, information, advice, and support, then they will not know what behaviours are expected of them, nor have the confidence to exhibit those behaviours. The behaviours that need to be ingrained in staff must also be agreed upon by leadership and understood at a senior level.

Think about how best to deliver and refresh security messages to all airport staff not just those that work in security, and to wider stakeholders (including the public) using various channels, such as:

- Electronic - email, apps, and the intranet;
- Print – posters, newsletters, or desk drops;
- Interactive security events and exercises;
- Face-to-face meetings such as staff briefings, airport pass collection, and training;
- Role profiles or job descriptions and regular performance appraisals and rewards schemes;
- Announcements, including public announcements if public messaging is part of your campaign; and
- SMS messages or a text service that allows staff (and the public) to report suspicious incidents discreetly and anonymously 24 hours a day.

Whichever mode of messaging is used, content and tone are crucial. Clear messaging that encourages personal responsibility will lead to improvements in behaviours. Resources which can be customized and used to support the establishment and maintenance of a robust security culture can be found in Part 2 of this document.

4. Retaining Buy-in

The **security manager** has a key role to play in generating and reinforcing security messages and communicating that they are the 'go-to person' for security concerns. The personal touch can help. For example, having the Head of Security quoted through internal communication channels saying just how much they valued a report-in from a staff member and what they did to action the report.

Staff, including junior staff, can also serve as ambassadors of positive security culture change for the next generation of aviation professionals, especially when appointed by senior management. Long term culture change happens when desired behaviours become the norm.

Practical tools that some organizations have used to good effect to promote a positive security culture and security awareness are:
- Lunchtime lectures by specialist speakers;
- Team meetings and awareness briefings/quizzes;
- Online articles on security and computer screen savers (that change every month);
- Special security events and days at airports;
- Downloadable podcasts, especially considering how people today are connected through mobile devices. Social media (Facebook, Twitter, Instagram, etc.) can provide opportunities to disseminate security awareness messages or videos;
- Glossy magazines and booklets;
- Blogs by senior security personnel about outcomes of suspicious activity reports and on items that staff may have seen in the media and what they mean for the airport (providing reassurance and encouraging vigilance);
- Annual security refresher training and role-specific security training and exercises; and
- Key Performance Indicators and the monitoring of them built into contracts of staff and contractors.

It is important that staff who already display good behaviour are acknowledged and encouraged to continue displaying such behaviour. Think about a rewards approach to motivate and maintain a good security culture. The traditional response to a security violation is punitive, and sometimes required. However, a reward approach to create and maintain buy-in can also have a positive change in behaviour. A simple example is handing out vouchers on a random basis for a coffee/snack redeemable at the airport when good security behaviour is observed.

Providing feedback to staff to encourage the desired action and discourage the undesired action is key to sustaining positive security culture. If staff receive little or no positive feedback when trying a new behaviour, or they associate the behaviour with a negative response, they may be less likely to perform the behaviour again. Staff may also be motivated by regular reports of actions taken as a result of their reporting of suspicious behaviours.

5. Communicating Methods

Identify key messages that need reinforcing based on current airport vulnerabilities and risks as well as the behaviours security staff are expected to follow. This could include messages on the importance of staff vigilance, pass wearing, and the reporting of suspicious behaviour.

Consider the timelines for communicating these messages to staff: are some necessary to promote as a staff member receives an airport badge? Do others require reinforcement over time?

Focus on messages that underpin your communication and repeat them to reinforce your priorities and embed understanding. Keep messages fresh and deliver the same message in different ways to stop threat fatigue.

Having the right message and medium to disseminate it is only part of the story. You must decide who will be the 'voice' of your campaign. Who has the greatest credibility? Who will make the message really resonate with staff?

A successful campaign relies on having key figures from inside the airport (as well as outside where appropriate, such as the local police or the security regulator) tell staff that their vigilance and reporting are important.

Different staff audiences might need **endorsement from different people.** For example, if you have a significant, cynical group of staff then you may consider that endorsement is best coming from a credible external expert. For new staff attending their airport induction course, the message may be best delivered by the Head of Security. Enthusiastic staff volunteers can also be very effective ambassadors, speaking to staff on their own terms.

6. Creating an Implementation Plan

Changing security behaviour requires leadership and a clear and coordinated strategy to ensure that interventions are consistent, practical and meaningful. Developing an implementation plan with clearly defined timelines, deliverables and responsibilities will assist in managing the **security culture campaign.**

This plan should include:
- Creating a campaign team, including a senior project manager and/or a visible champion who will take ultimate responsibility for campaign delivery;
- Clarifying the aims and vision of the campaign, including a timeline for implementation and ways to measure impact;
- Bringing in a culture change specialist who would have views on how to manage security as an integral part of the business and apply best practices in approaches and principles e.g. changing procurement models, the role of the Board, cross discipline recruitment, cybersecurity;
- Identifying a budget and resources, as well as assessing who might sponsor the campaign, such as a security partner or agency;
- Including wider security messages and including the Airport Security Manager as part of the campaign team;
- Communicating and liaising with key stakeholders, including existing staff at airports and air carriers, third party contractors, law enforcement agencies, and others, as appropriate, so that messages can be agreed upon and disseminated;
- Measuring the campaign's impact and how to report progress to the Board or CEO;
- Determining whether you can embed the campaign into long-standing packages such as inductions or security training; and
- Identifying timelines and/or milestones to refresh the campaign.

7. Evaluating Implementation

The ability to review and amend your security culture campaign is very important, both to identify the parts that work and those that do not. There is no point in sending out a message that people ignore.

Think about where you put up materials and evaluate how well they are working. Speaking to staff and/or conducting a short feedback questionnaire or survey will give you a good sense of how visible the materials are and whether they have changed staff behaviour and resulted in positive security culture and increased vigilance.

Typically, posters should be up for short period of time before they are rotated so that they don't start to fade into the background as staff become too familiar with them. About a week into the campaign you could consider other activities to reinforce the message – for example, getting security officers to hand out wallet cards and/or lanyards to staff as they enter or exit the site. Interactive material like training films with the opportunity for staff to discuss and comment are also helpful, as are computer-based learning packages.

Punctuate the big impactful visual elements of your security culture campaign with:
- a report on the outcomes of the campaign so far – how staff received it – with recommendations for improvement;
- regular security blog updates from the Head of Security; and
- relevant public news articles to remind staff of the need to be vigilant and report in.

8. Responding to Suspicious Activity and Incidents

Giving people a variety of options in how they report suspicious activity is useful; text/sms, telephone, or speaking to someone in person maximizes the chances that suspicious activity will be reported. Anonymous reporting or "whistle-blowing" where people can report incidents of poor behaviours can be useful. Incidents can then be addressed without the fear of repercussions.

How you respond to reported security incidents and occurrences is important, and where possible you should try to publicize any successful outcomes. Staff will take encouragement from learning that their actions have led to a good security result.

It is also important that those who receive threat information are properly trained and have threat reporting and evaluation systems at their disposal. This will help to raise vigilance and security awareness.

Incident response – awareness is part of security culture, and security culture is part of incident response. Consider holding lessons learned exercises post security incident to determine strengths and weaknesses that should be addressed to increase response effectiveness and to improve the security culture campaign.

Part 2 - Customizable Resources

This section contains templates and information to create a practical security culture campaign that can be edited to suit your local airport environment or organization:

1. Posters stressing the importance of security culture, including wearing badges, reporting security incidents, and vigilance
2. Wallet cards and pamplets for airport pass holders: reporting security incidents
3. Sample security culture knowledge checklists
4. Sample security awareness quiz for entrance into restricted areas (pass holders)
5. Security awareness and security culture videos, messaging and presentations
6. Scripts for public security announcements
7. Key Performance Indicators on the implementation of security culture
8. Questions to access the status of security culture

# GUIDE TO THE RUNNING OF A SECURITY CULTURE CAMPAIGN

PART 2 – CUSTOMIZABLE RESOURCES

This section provides a number of practical tools that can be used to help develop a security culture. It includes the following materials:

1. Posters stressing the importance of security culture (Pages 9-17), including:
    - Proper procedures for wearing airport ID/passes.
    - Information to report security incidents.
    - Promoting vigilance and action.
    - Identifying reporting procedures for unattended items and suspicious activity.

2. Wallet cards and pamphlets for airport pass holders with information on how to report security incidents (Page 18-20)

3. Sample security culture knowledge checklists (Page 21)

4. Sample security awareness quiz for entrance into restricted areas (pass holders) (Page 22-23)

5. Security awareness and security culture videos, messaging and presentations (Page 24-27)

6. Scripts for public security announcements (Page 28)

7. Key Performance Indicators on the implementation of security culture (Page 29)

8. Questions to assess the status of security culture (Page 30)

NO PASS, NO ACCESS
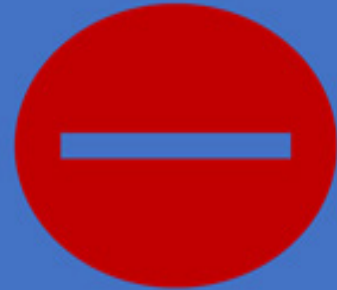
CHALLENGE ANYBODY WHO IS NOT WEARING A PASS

UNUSUAL BEHAVIOUR?
TOO MANY QUESTIONS?
LOITERING?
DOES SOMETHING NOT FEEL RIGHT?

REPORT IT ON

CALL: _____

KEEP YOURSELF AND OTHERS SAFE

When in Doubt Check it Out

Security is everyone's responsibility

Together, we've got it covered.

Do you know what suspicious activity looks like?

Do you know what to do if you see something out of the ordinary?

Remember, being seen to be vigilant and ready to engage with the public can also help deter criminals.

Police Response (the 5 W's)

- What is it?
- Where is it?
- When was it found?
- Why is it suspicious?
- Who are the witnesses?

HOT Protocol (for Unattended Items)

- **H- Hidden**
  - Not in general view and may have deliberately been positioned in a discrete area
- **O- Obvious**
  - This is when the item is obviously suspicious, signs of tape, wiring, batteries, etc.
- **T- Typical**
  - Not typical of the normal, everyday situation; out of the ordinary

If in doubt, DON'T ignore it. Tell your supervisor. Call your control room IMMEDIATELY on

Together, we've got it covered.

Suspicious Activity

Always be vigilant for people:

- Hanging in or around restricted areas
- Taking an interest in CCTV cameras
- Closely watching all staff movements
- Appearing highly agitated and nervous

You know what is normal. Trust your instincts. Report any suspicions IMMEDIATELY. In doing so you are helping to ensure your safety and the safety of those around you.
Don't forget the power of a simple "Can I help you?"

Are they checking security?

Notify staff or call police

SEE IT. SAY IT. SECURE IT.

TOGETHER, WE'VE GOT IT COVERED

Are they trying to hide something?

Notify staff or call police

SEE IT. SAY IT. SECURE IT.

TOGETHER, WE'VE GOT IT COVERED

Seen something suspicious?

Don't be afraid to tell us.

Notify staff or call police

SEE IT. SAY IT. SECURE IT.

TOGETHER, WE'VE GOT IT COVERED

Do they look worried about what we might find?

Notify staff or call police

SEE IT. SAY IT. SECURE IT.

TOGETHER, WE'VE GOT IT COVERED

UNUSUAL BEHAVIOUR OR ACTIVITY?

CHALLENGE AND REPORT
WHAT? WHERE? WHEN? WHO? HOW?

CALL: _____

YOUR INTERVENTION COULD SAVE LIVES

SECURITY BREACH?
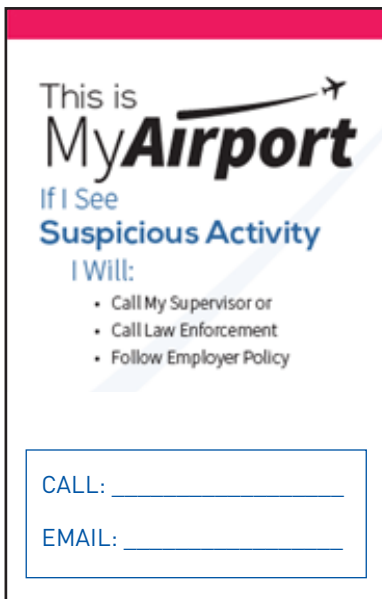## LOST OR STOLEN PASS OR
EQUIPMENT?

DON'T DELAY

CALL: _____

This is
My**Airport**

I am the
EYES
EARS and
VOICE
of my airport

Suspicious
Activity

if you
SEE | SAY
something | something™
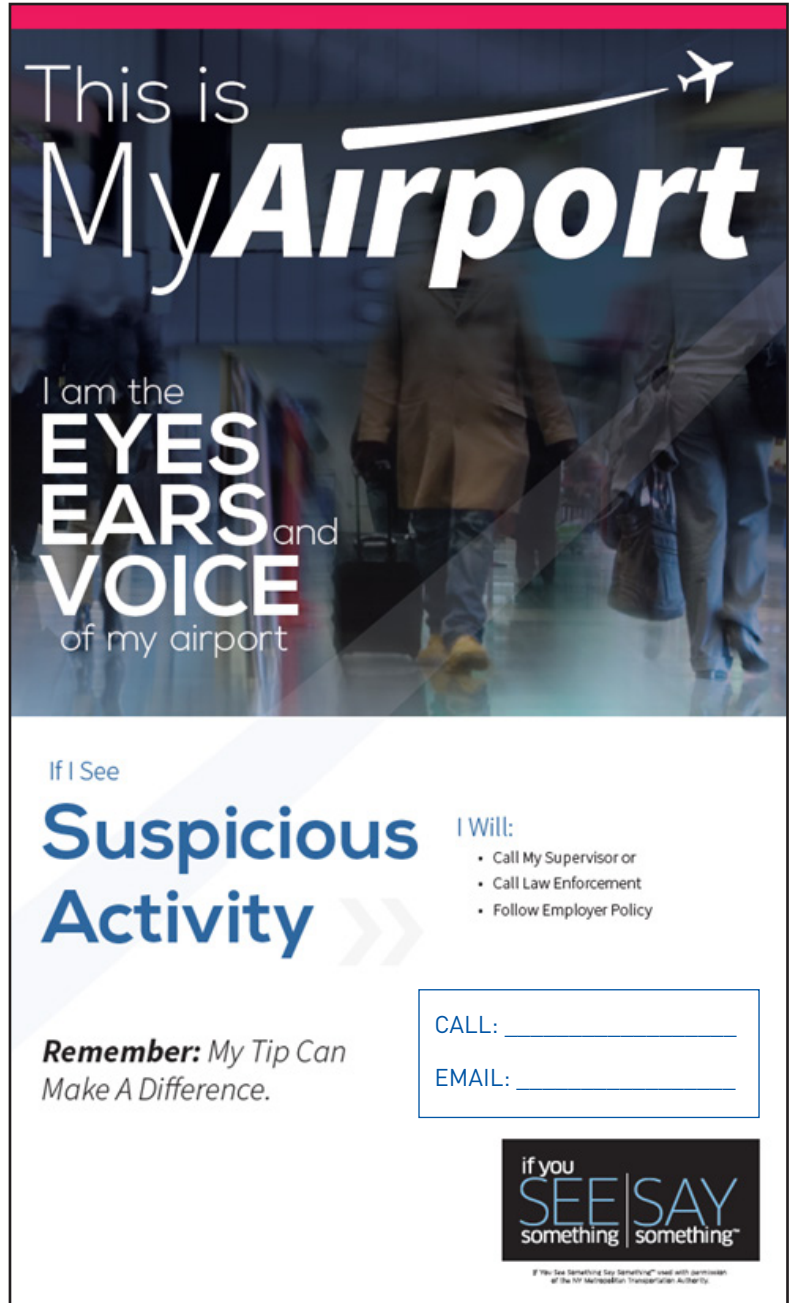
This is
My**Airport**

If I See
Suspicious Activity
I Will:

- Call My Supervisor or
- Call Law Enforcement
- Follow Employer Policy

CALL: _____

EMAIL: _____

This is
My**Airport**

I am the
EYES
EARS and
VOICE
of my airport

If I See
Suspicious
Activity »

I Will:

- Call My Supervisor or
- Call Law Enforcement
- Follow Employer Policy

Remember: *My Tip Can Make A Difference.*

CALL: _____

EMAIL: _____

if you
SEE | SAY
something | something™

This is MyAirport

If I See
Suspicious Activity

I Will:
- Call My Supervisor or
- Call Law Enforcement
- Follow Airport/Company Policy

Insider Threat
Report It!
It is your responsibility!

CALL: _____

EMAIL: _____

Remember:
My Tip Can Make A Difference.

This is MyAirport

Suspicious Activity

if you
SEE | SAY
something | something™

What is an Insider Threat?

An insider threat is one or more individuals with access and/or insider knowledge that allows them to exploit vulnerabilities of the nation's transportation systems with the intent to cause harm.

These are the people we may work with or around every day. Insiders include current and former airport and airline employees, contractors, vendors, construction workers, or others that have access and/or knowledge.

The majority of employees are low risk and pose no security threat. But, we must remember, some insiders do have ill intent.

An Evolving Threat

Those who seek to threaten airport security may be employed at the airport. They exploit their position, seek out, and recruit other potential insider support.

Airport employees are extremely attractive to them as they have current knowledge of security protocols and are aware of airport vulnerabilities.

Terrorist groups want insiders to assist with information for their plans, increasing the likelihood of success.

Identifying Potential Insider Threats

As an airport employee, how can you identify potential insider threats?

There are several key personal motivators and key behavioral indicators that can identify potential sources of insider threat in co-workers at the airport.

Personal Motivators:
- Divided Loyalties
- Ideological or self-identity shifts
- Change in attitude, morale or work ethic
- Seeks adventure and thrills
- Vulnerable to blackmail
- Feelings of anger or revenge
- Greed or financial need

Behavioral Indicators:
- Disregard for security policies
- Conducting unauthorized searches
- Social Engineering
- Suspicious foreign contacts or travel
- Enthusiastic interest in specific airport security measures
- Working unusual hours without authorization

Importance of Vigilance

Insider threats are real and pose significant risk to our lives and our nation.

They can take days, months, or even years to plot. They can involve one or multiple individuals. They can have the potential to impact dozens of people or thousands.

Potential consequences of not reporting:
- Violence or terrorist attacks
- Loss of property, financial assets, and sensitive information
- Delays, obstacles and work stoppages
- Damage to reputation

You are the **Eyes**, **Ears**, and **Voice** of your airport. What you observe can save lives.

Reporting Process

If you identify potential insider threats, report the incident or behaviors to your supervisor, law enforcement, or follow airport/company policy.

When reporting what you observed, be as descriptive as possible. Include:
- Who you saw
- What you observed
- When - date and time
- Where - location it occurred
- Why you believe the activity or behavior to be suspicious.

if you
SEE | SAY
something | something™

Sample security culture knowledge checklists

1. **Select the best answer: Holders of an Airport Temporary Identification Card (Airport Pass) must:**
   a. Return their identification card when it is no longer needed
   b. Familiarize themselves with security requirements and their responsibilities
   c. Remain in line of sight of their security escort at all times when airside
   d. All the above

2. **Select the best answer: What should a staff member do when required to be screened by the screening agency at a non-passenger screening location?**
   a. Politely refuse screening and proceed into the Security Restricted Area
   b. Comply with the screening procedures
   c. Turn back and try entering again at a later time
   d. Suggest screening is not required if access control permissions exist

3. **Select the best answer: A staff member notices a worker in the Security Restricted Area who is not displaying airport identification. Who is responsible at this moment for either reporting or asking that individual to display their airport identification?**
   a. Airport Security Officers
   b. Staff member
   c. Airport Police
   d. All the above

4. **Select the best answer: The Security Restricted Area is best described as?**
   a. The entire airport
   b. Public meet and greet areas
   c. Passenger boarding lounges and concessions areas
   d. Areas located post security in the Terminal and outside on the ramp/airfield. Only authorized persons may enter this area when they have appropriate valid airport identification and work-related duties.

5. **Select all that apply: Taking shortcuts in security or failing to abide by the security rules and regulations of the airport may result in:**
   a. Operational disruption and increased cost
   b. Confiscation of security privileges and criminal prosecution
   c. Lack of public confidence
   d. Negative media attention
   e. None of the above

6. **True or False: Access control passes can use a colour coding system and/or a numbering system specific to each airport that specify the security areas staff are permitted to access and work in?**
   a. True
   b. False

7. **Select the best response: A staff member comes to a security door and scans their airport identification but the door remains locked and the card reader flashes red. They should:**
   a. Contact airport security or the access control (pass office) for assistance
   b. Call the local police department to grant them access
   c. Force the door open as this is a mechanical issue
   d. Wait for another staff member who has access to this door and follow behind them

Answer Key:
1. d
2. b
3. d
4. d
5. a, b, c, d
6. a
7. a

Sample quizzes which all airport workers could take before collecting their airport passes.

Online security awareness courses could be developed which all pass holders would need to take prior to obtaining an airport identification card (airport pass). Alternatively, quizzes could be developed which include, but are not limited to, dos and don'ts with airport passes and basic protocols when encountering security incidents. For example:

Access to Airside or Security Restricted Areas:

1. **When are you authorized to use your airport identification card to gain access to airside or security restricted areas?**
   a. When on duty and only if you have a legitimate business reason for entry
   b. To meet family and friends
   c. To meet celebrities

2. **Are you allowed to ask a passenger to help you to buy liquor and cigarettes in the airside or security restricted areas if you are not travelling?**
   a. Yes
   b. No

3. **If you forget your airport identification card can you borrow your friend's identity card?**
   a. Yes
   b. No

4. **Once you have entered the airside or security restricted area is it mandatory to always display your airport identification card?**
   a. Yes
   b. No

5. **If you see someone acting suspiciously in the airside or security restricted area what should you do?**
   a. Ignore him/her
   b. Inform the relevant authorities using local reporting procedures
   c. Confront him/her yourself

6. **You know that your friend is not working today but you saw him shopping and eating in the transit area. What should you do?**
   a. Inform authorities
   b. Confront him yourself
   c. Act like you saw nothing

7. **If you find a defective card reader, lock, door or gate what action should you take?**
   a. Report to relevant authorities
   b. Ignore
   c. Try to fix the problem yourself

8. **If you have problems with your airport pass when exiting or entering the airside or security restricted areas what should you do?**
   a. Ask your friend to use their airport identification card
   b. Report the problems to your card issuing authority (office)

Unattended Bag

9. **If you see an unattended bag what should you do?**
   a. Ignore it
   b. Do not touch/open the bag and look around for the owner. If unsuccessful, report it immediately to the appropriate authority following your local reporting procedure.
   c. Touch the bag and take it to lost property

Use of Airport Identification Card / Airport Pass

10. You realize that you lost your airport identification card. What should you do?
     a. Ignore it and do nothing
     b. Borrow someone else's card
     c. Follow the local reporting requirement for lost passes

11. When should you consider replacing your airport identification card?
     a. When you change job and your access requirements change
     b. When your photograph on your airport identification card no longer matches your appearance
     c. Both of the above

12. When must you return your airport identification card?
     a. When it has expired or is cancelled
     b. On request of any security official
     c. Both of the above

13. What should you do if you no longer need an airport identification card?
     a. Destroy the card securely
     b. Return the card to your employer so it can be returned safely to the card issuing authority for cancellation
     c. Give your card to someone else who could use it

Airport Pass Zones

14. How do you know what areas you are authorized to access?
     a. Try to use your identification card at the access point
     b. Consult the numbers and colours shown on your identification card
     c. Ask a colleague

Security Awareness and Security Culture videos, messaging and presentations

Encourage all staff to watch general security awareness and security culture videos.
For example, IATA 'See it Report It' videos can be downloaded[1] at https://sems.iata.org/

Another example are the videos provided by Vancouver International Airport and can be accessed via the following links on:
• Reporting Unattended Items: https://youtu.be/mmDf3p11ioA
• Misuse of Airport Identification Cards: https://youtu.be/MiBWK6cPaXI
• Maintain Care and Control: https://youtu.be/K2tMZYd-HAA
• Staying With Your Bags: https://youtu.be/Eq7cja315Z0

[1] On the SiRi portal 1) Go to REGISTER to create a profile; 2) Go to the 'See it Report it' window; 3) Highlight one of the two videos: awareness or reporting 4) When the video starts, if you right-click then select "Save video as ..." you can download the video in HD format.

The following is an example of a message from an Airport Security Service highlighting a security awareness campaign, as well as the accompanying slide deck that was provided to security managers.

Security Awareness

Dear security managers

Security Services is running an Awareness campaign from 22 October to 4 November with the key message that when we are aware – and act – we keep our airport secure.

During the two campaign weeks, we encourage your company to help us spread the Awareness message to your employees. For this, we have made a short, 2-minute film, which focuses on:

- Unattended luggage
- Visible ID card/tailgating
- Blocked emergency exit
- Unauthorized access

We enclose a PowerPoint presentation that you can use on your briefings and/or send to your employees. It contains a link to the film on YouTube and highlights the Awareness principles. We also encourage you to discuss the following with your employees:

- **What is tailgating*?**
- **What can *you* do to prevent tailgating?**

To bring attention to the campaign you will see the enclosed poster (only in Danish) in various break rooms and staff entrances, and you are welcome to print it yourselves and hang where you would find it relevant for your employees.

Last, but not least, we encourage your employees to participate in our contest to win a dinner for 2. All you have to do is answer a question after watching the Awareness film. We draw the winners in the week after the campaign.

We thank you in advance for your participation and support to spread the principles of Security Awareness. As always, we welcome your feedback via email: sec-awareness@cph.dk.

Best regards,

Henrik W. Gericke
Chief of Staff
Security Policy & Regulation, Security Services

*Tailgating means that one or more persons without access follows you in/out after you have used your ID-card
- *If you use your CPH ID card to open a door to a secure area you must ensure that people who follow you have an CPH ID-card (or are accompanied by a person with CPH ID card)*
- *Ask to see other people's CPH ID card if you can't see it and you are the one opening the door*
- *Watch the door close to ensure that persons without access do not enter nor exit*
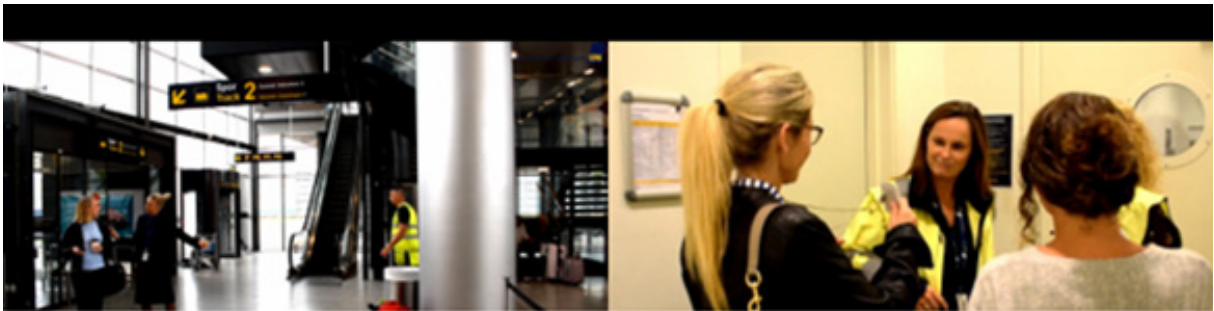
→ **Awareness on your way through the airport**
Security Awareness Campaign
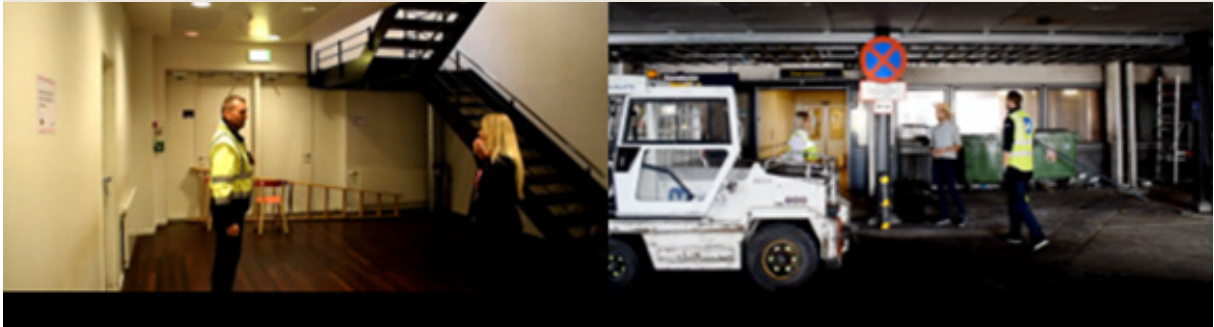
Awareness on your way through the airport
See and report – call OC

Security Awareness
Campaign 2015

→ Always respond to:

- Unattended luggage
- Visible ID card/tailgating
- Blocked emergency exit
- Unauthorized access

→ Security Awareness campaign

Security Awareness

When we are aware, we keep our airport safe and secure

Public Announcement Scripts

Public security announcements can build vigilance and raise awareness of security issues.

Example 1: An audio message saying: **"See It. Say It. Secure it."** could be played at regular intervals for passengers travelling to and arriving at airports. This could be supplemented by posters promoting the message: "See It. Say It. Secure it."

Script. "*If you see anything unusual or suspicious please report it to airport staff on xxxxxx. "See It. Say It. Secure it."*

Example 2: An audio message saying *"Security is everyone's priority. If you see something suspicious, please report to airport personnel"* to help build vigilance and raise awareness of security issues.

Key Performance Indicators (KPIs)

Security KPIs can be built into contracts of staff and contractors who are involved in the provision of airport services to promote security culture and security awareness:

1. **Training -** the service provider is required, on a regular basis, to provide security awareness and/or related training and conduct tests to its staff/contractors to ensure that they understand the applicable security standards and procedures that apply to them;

2. **Signing -** the service provider's staff sign a written document to confirm they have (i) read, understood and agree to comply with the security standards and procedures; and (ii) participated in and passed the relevant security training session(s);

3. **Monitoring and Supervision -** the service provider must actively monitor and manage the delivery of the services to ensure that it complies with the terms of agreement, as well as the security standards and procedures;

4. **Culture -** the service provider will develop and maintain an organizational culture *where a security comes first philosophy* forms the basis of all workplace activities by its staff;

5. **Organization -** a security manager / managerial staff shall be appointed to maintain efficient and effective communication, and ensure the required security standards are met. Similarly, a dedicated supervisory staff shall be appointed, for each shift, to handle real security related issues;

6. **Standard Operating Procedures (SOPs)–** SOPs shall be developed to clearly list the security work process and a complete review shall be made at least once a year;

7. **Contingency handling -** the service provider shall have contingency plans established;

8. **Communication –** the service provider will set up regular meetings with the requested company to review security incidents at least once every quarter and set up procedures to report security incidents.

Assessment of the Status of Security Culture
Assessing Security Culture – question set

To assess if an effective security culture exists within your organization, the following questions may be asked:

1. Is security an organization priority and a core value of the airport?

2. Are policies and procedures in place that define security culture, i.e. a Vision/Mission Statement with a description of what effective security looks like?

3. Do staff know how their work contributes to the overall security of the airport and its users?

4. Are security threats and risks properly understood at all levels (up to and including senior managers)?

5. Do managers promote an effective security culture by visibly endorsing and executing security initiatives and leading by example?

6. Are there written records of agreed security standards and procedures? And are these records easily accessed by staff?

7. Are staff given the resources and time that they need to comply with security measures?

8. Are all staff appropriately and regularly vetted?

9. Are staff airport passes visible at all times? And if not, are staff being challenged for not displaying their passes?

10. Do all staff and passengers pass through security screening?

11. Do training materials (including refresher training materials) contain a description of the current threat and security processes?

12. Does training build in security culture best practices?

13. Are there posters and/or other communication campaigns around the airport promoting positive security behaviours, reminding staff and visitors to remain vigilant and to report suspicious activity immediately?

14. Do management communicate with all staff on security issues through written communications and staff announcements?

15. Are security messages part and parcel of airport communications (internal and external), including deterrent communications?

16. Are processes in place to enable and encourage staff to report security-related incidents (with the option of anonymity)?

17. Are staff provided the opportunity to suggest ways in which security could be improved e.g. through staff surveys (question sets), feedback boxes, interviews, workshops, peer reviews?

18. Is there a process that provides regular (at least annual) feedback to security officers on their work programme?

19. Do staff (including security officers) receive recognition from managers for positively contributing to security?

20. Is there good cooperation, support and communication within teams of security officers? And do security officers and managers consider themselves to be part of a team?

Part 3 – The ICAO Toolkit on Enhancing 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.

> Developing and sustaining a positive security culture is an essential component of a robust and effective security regime. It can help mitigate against a range of risks that could cause fatalities and casualties and operational, reputational or financial damage.

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 ° OACI ° ИКАО | ICAO

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:

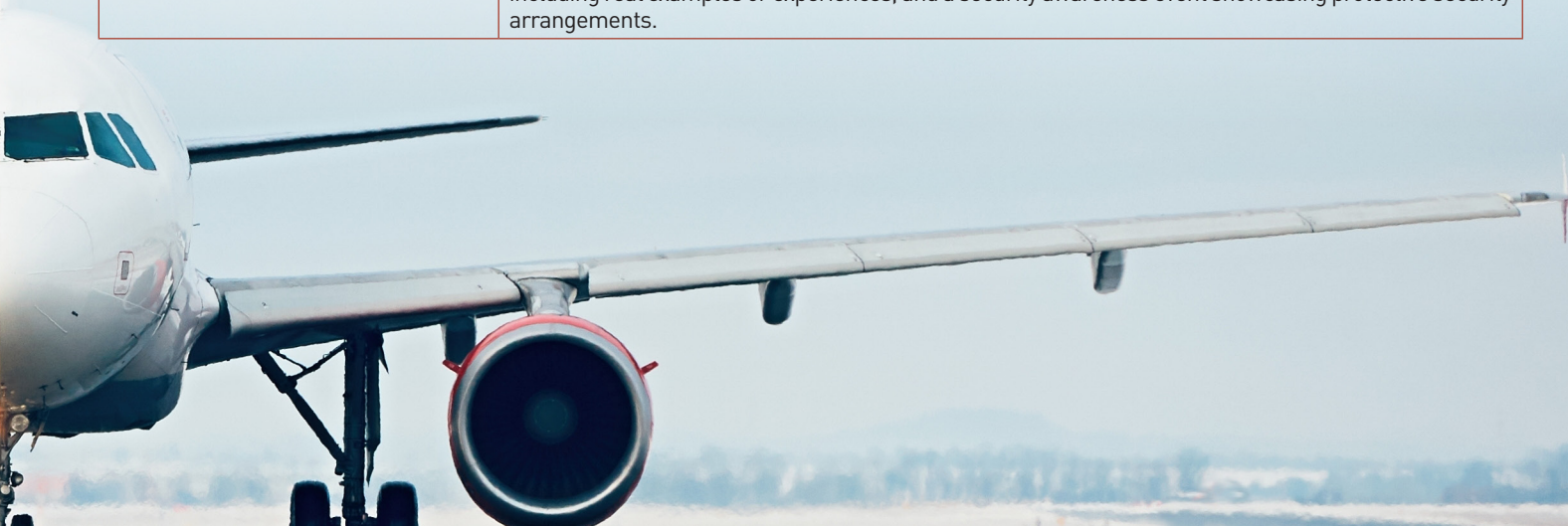| POSITIVE WORK ENVIRONMENT	
DESIRED OUTCOME	TOOLS
A work environment which drives and facilitates a positive security culture.	Clear and consistent: policy, processes, systems and procedures – enshrine security in all corporate policy and procedures, including those areas which do not have a primary 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.

ICAO