Aviation Security Culture

Air Macau Security policy

Safe flight

Endorsed by CEO

Continues improving

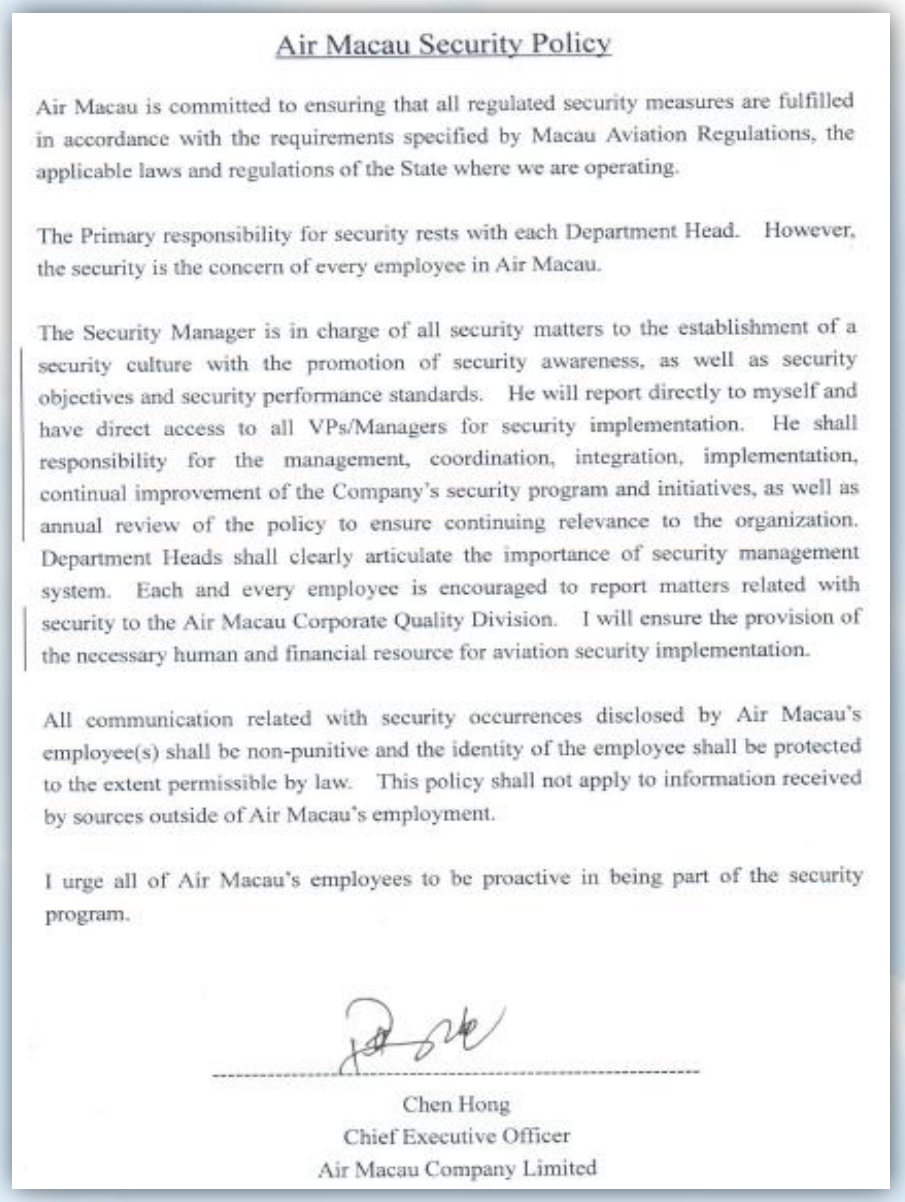
Unified policy

Report whenever you suspect

Information sharing

Training

You & me



Air Macau Security Policy

Air Macau is committed to ensuring that all regulated security measures are fulfilled in accordance with the requirements specified by Macau Aviation Regulations, the applicable laws and regulations of the State where we are operating.

The Primary responsibility for security rests with each Department Head. However, the security is the concern of every employee in Air Macau.

The Security Manager is in charge of all security matters to the establishment of a security culture with the promotion of security awareness, as well as security objectives and security performance standards. He will report directly to myself and have direct access to all VPs/Managers for security implementation. He shall responsibility for the management, coordination, integration, implementation, continual improvement of the Company's security program and initiatives, as well as annual review of the policy to ensure continuing relevance to the organization. Department Heads shall clearly articulate the importance of security management system. Each and every employee is encouraged to report matters related with security to the Air Macau Corporate Quality Division. I will ensure the provision of the necessary human and financial resource for aviation security implementation.

All communication related with security occurrences disclosed by Air Macau's employee(s) shall be non-punitive and the identity of the employee shall be protected to the extent permissible by law. This policy shall not apply to information received by sources outside of Air Macau's employment.

I urge all of Air Macau's employees to be proactive in being part of the security program.

Chen Hong
Chief Executive Officer
Air Macau Company Limited

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 is Everyone's Responsibility

Security Culture must be developed and promoted **from TOP to DOWN.**

From **Top Management** to **all departments** to **all staffs**.

All staff should understand the nature of the threats that everyone and the organization face. Without this awareness, there will be a lack of desire to embed a positive security culture.

Security belongs to **everyone** and bakes security into **everything** they do.

Security is Everyone's Responsibility

Every staff has significant role in the Security Program
所有員工在保安計劃中都有要職

Operational staff performs security duties
前線員工執行保安職責

Management, back office staff offers support to each staff when performing security duties.
(e.g. legal, human resources, hardware / software, financial and training, etc.)
管理層、後勤員工為前線員工提供支援

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 may more vulnerable to social engineering

Insider cases are often linked with a poor security culture

First impressions count; the organisation may be perceived as an easy target

Benefit of Security Culture

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 behaviors/activities of concern;
- Employees feel a greater sense of security; and
- Security is improved without the need for large expenditure

Insider Threat

What is insider threat?

Any individual with inside knowledge or access has the **potential to harm** the organization and its people.

The threat may be come from full or part-time permanent employees, individuals on attachment or secondment, contractors, consultants, agency staff, temporary staff or staff from **other organizations** .

Different kind of Insider Threat

Malicious 惡意: Employees who aim to hurt their organization or their colleagues. Ego, personal advantage, money, political or religious belief.

- Theft (of information), Violence, terrorism(support), espionage, helping others to get illegal access, Selling information to criminals

Negligent 過失 : Employees who are aware of security policies and procedures but decide to bypass them.

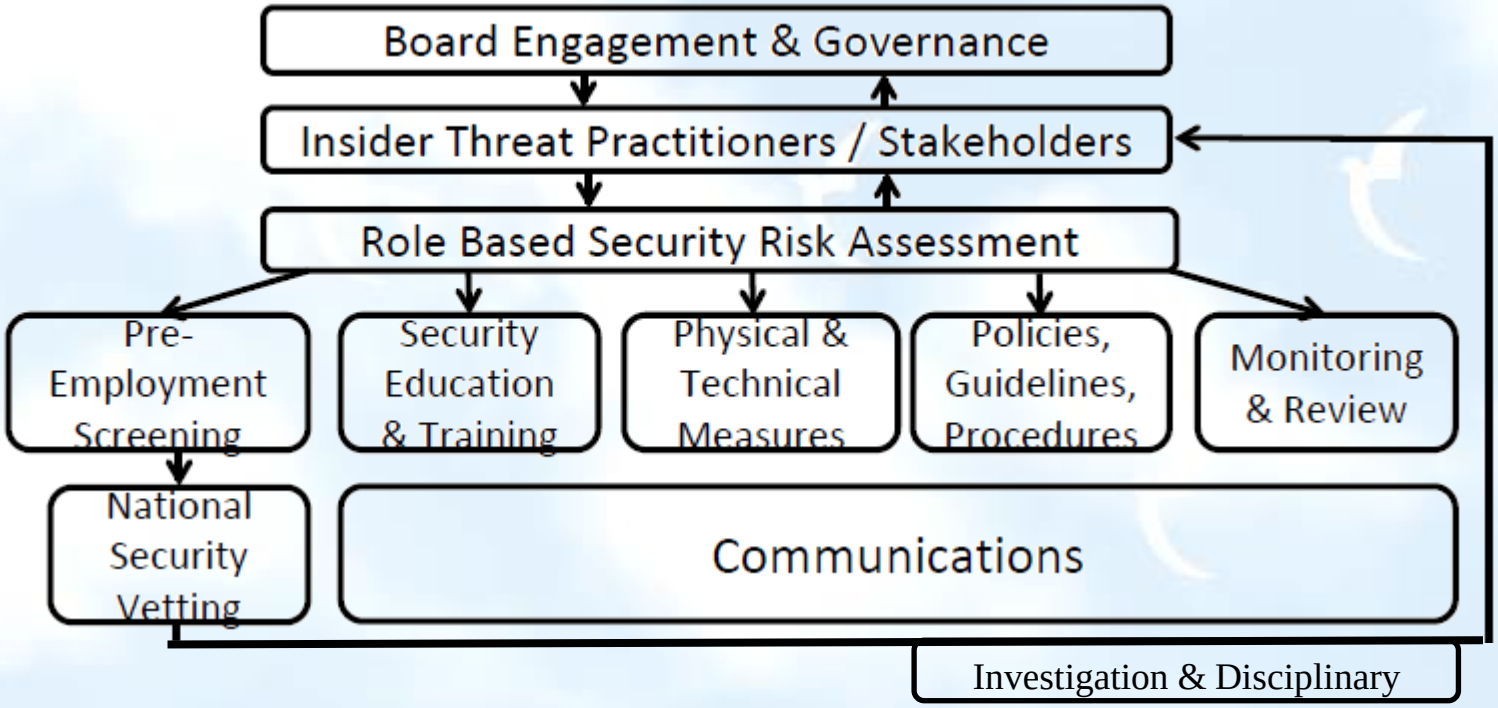
- Lend badges to colleagues.
- Illegal copying of information to personal devices.
- Share passwords.
- Authorization of visitors without airport ID cards or without escort.

Accidental 意外: Employees who are aware of security policies and procedures but accidentally bypass them.

- Forgetting procedures,
- Accidentally sending information to wrong person.
- Sharing access and/or passwords.

Mitigation of Insider Threat

Insider Threat
gation Framework



How to manage the insider threat effectively?

Mitigate Risky Behaviour

- Train and notify staff members of policy violations when they happen.
- Restrict access to confidential assets and information/data based on individual functions (need-to-know access rights).

Know Your Employees

- Perform structured pre-employment checks.
- Set up a system of infinity/ continuous screening.
- Train staff and contractors on company security/ confidentiality policies.

Monitor Behaviour

- Identify staff violating policies/procedures.
- Identify staff abusing or misusing data, services and privileges.
- Inquire about hazardous behaviour.

Know Your Assets

- Establish a list of the company's critical assets (incl. data, facilities, equipment and services).
- Evaluate impact.

Sharing information is key, as an alarm signal in one department cannot be known in another department….

(red flag alarm)

Case Study-Unsuccessful terrorist plot in Somalia

Daallo airlines 159, 2016

https://www.youtube.com/watch?v=i_DAXMImSBc

Case Study-Unsuccessful terrorist plot in Somalia

Incident Summary:

In 2016, airport employees handed a laptop containing an explosive device to a passenger. Activating and explosive device at high altitude would have brought the plane down, killing all 74 passengers and crew.

Harm done:

Two persons injured onboard the aircraft.

One casualty (the person carrying the explosive device).

Breach in the fuselage of the Daallo Airlines airplane.

You are the eyes and ears of Air Macau

You can help protect NX and the people around you.

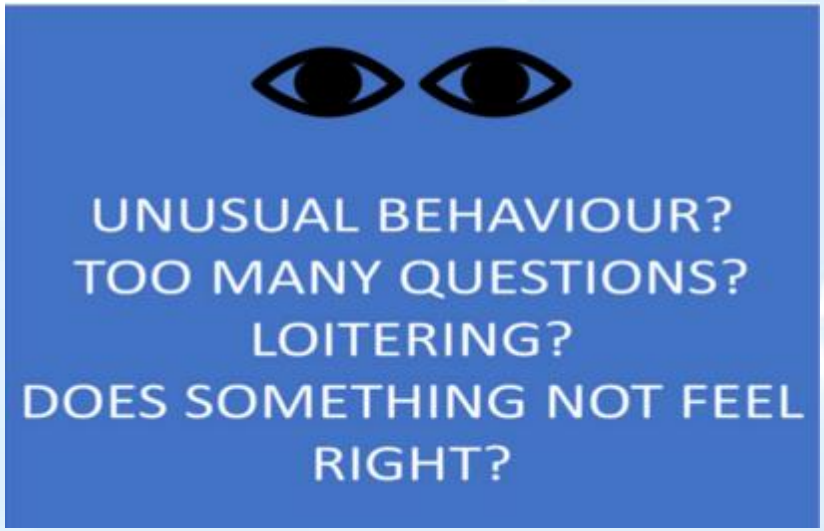
How to do ?

- ✓ Follow security measures at all times.
- ✓ Speak up if colleagues neglect security measures.
- ✓ Speak up if there are no security measures, or if they are not strict enough.

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.



Reporting

Encouraging reports

Reporting mechanisms are a key part of a strong security culture – reporting helps to understand what is going on in security. A strong culture also supports peers challenging one another when security processes are broken/ignored.

Reporting time frames – Initial reporting

From time of incident / threat	SMS or telephone	To	Within
Reporting entity	→	AOC-OCC	• 15 min for levels 3 & 4 • As soon as practical for levels 1 & 2
↓			
From time of Information of reporting entity			
AOC-OCC	→	CAM-AOD	• 15 min for levels 3 & 4
↓			
From time of Information of AOC-OCC			
CQD	→	AACM	• 15 min for levels 3 & 4

Reporting time frames -Follow up written report

From time of incident / threat	Submit written report	To	Within
Reporting entity	→	CQD	• 24 hrs for levels 3 & 4 • 48 hrs for levels 1 & 2
↓			
From time of incident / threat			
CQD	→	AACM	• 48 hrs for levels 3 & 4

Report whenever you suspect

If you see something that doesn't look right

Written reports shall be submitted via any of the following forms:

- Security Incident/Event Report – SPM Annex 8
- Other AMU controlled forms if SPM Annex 8 is unavailable-Captain's report, Cabin Crew report or other divisional forms.

A. Initial reporting to AOC-OCC by either in person, telephone, VHF Transmission, SMS, ACARS or other prompt and practical means; and

B. Follow-up written report with relevant document (as available) to CQD thru:

1. E-mail (security@airmacau.com.mo); or
2. Fax (+853 8396 6522); or
3. OCS (MFM-HDQ-18A, CQD)

We'll sort it.

See it. Say it. Sorted.

JUST CULTURE
because we are all humans

Information sharing

Each Security Monthly Meeting Report including the Global Aviation Security Awareness is available in the intranet's Corporate Quality Center after each monthly meeting.

Staff are encouraged to address any feedback and comments, through local GM or directly, to the undersigned via email. Additionally, constructive contribution to the publication is welcome by all staff, especially significant topics related with security within respective jurisdictions.

Security belongs to everyone and bakes security into everything they do.

Thank you !