



# TECHNICAL GUIDANCE MATERIAL

## for

# Aviation Security Cybersecurity Culture Programme

**SUBJECT:** TECHNICAL GUIDANCE MATERIAL FOR AVIATION SECURITY CYBERSECURITY CULTURE PROGRAMME

**EFFECTIVE DATE:** 28 March 2022

### APPLICABILITY:

The guidance material is applicable in all aviation security operations with the aims to support aviation operators in designing and implementing a robust cybersecurity culture within their organizations.

### PURPOSE:

This TGM's serve to guide and support the aviation industry in developing an effective and resilient civil aviation cybersecurity programme. Through establishing a cybersecurity culture, which provide a commonly understanding defined based on set of assumptions, attitudes, beliefs, behaviours, norms, perceptions, and values that are inherent in the daily operation of an organisation and are reflected by the actions and behaviours of all informed by their interaction with digital assets.

### REQUIREMENTS:

The aviation industry to develop and cultivate cybersecurity culture that is inclusive and reflective of the industry security needs. Through incorporating pragmatic solution to educate with cyber awareness initiative , to ensure preparedness against possible cybersecurity attacks.

### 1. REFERENCES

- i. Aviation Security Manual -Doc 8973
- ii. ICAO Cybersecurity Action Plans (CyAP)-2021
- iii. TGM for the development of aviation cybersecurity programme

### 2. ABBREVIATIONS:

ABBREVIATION	DESCRIPTION
CSIAD	Critical Systems, Information, Assets, and Data
CyAP	Cybersecurity Action Plan
FAQ	Frequently asked question

### **3. GENERAL**

- 3.1** This TGM is responsible to guide aviation industry in formulating a cybersecurity programme, by establishing a proactive approach necessary to address the eminent multi attack vectors that has the ability to penetrate the decentralised aviation landscape. The cybersecurity culture programme is designed in line with the stipulated priority action intended to :
- a. Establish effective leadership, governance, and regulations.
  - b. Secure information infrastructure system
  - c. Information privacy and data security management
  - d. To adopt a cybersecurity risk management approach to aid in decision making and for accountability  
Increased awareness and development of cybersecurity culture.

### **4. THE PRINCIPLES OF CYBERSECURITY CULTURE**

- 4.1** The cyber security culture within the organisation may be defined as a set of knowledge, norms, values, assumptions of the staff that directly reflect their behaviour in dealing with the information technology and protecting the Critical Systems, Information, Assets, and Data (CSIAD).
- 4.2** The achievements to implement the stipulated priorities, required that a cybersecurity culture is developed to support the security and resilience of civil aviation against cyber threats and risks. Moreover, considering the role of the human in cybersecurity, a positive cybersecurity culture aims encapsulate parts of the organisation habits, conducts, and processes, by embedding them in daily operations as reflected by the actions and behaviours of all staff.
- 4.3** Cyber security culture should be an integral part of one's organisation and staff. Successful cyber security culture will shape the security thinking of one's staff and improve resilience against cyber threats and will allow one to effectively perform strategy goals without imposing burdensome security steps. Defining a minimal cyber security culture within one's organisation is a process that requires a multithreaded approach and commitment not only from the senior management but also down to junior levels.
- 4.4** A well-established cyber security culture is not only an awareness of behaviours, norms, and values, but it is also a mutual understanding between senior management, people responsible for the cyber security implementation, and the entire staff about their responsibilities and practices to defend CSIAD against the cyber-attack.
- 4.5** The establishment of a strong and effective cybersecurity culture is an integral part of an organisational and staff culture, with the goal of improving the overall performance and resilience against cyber threats
- 4.6** The core elements of an effective organisational aviation cybersecurity culture are captured below to provide to guide aviation organisation in the implementation of its cyber culture.
- 4.7** However, although these core elements are well defined, cybersecurity culture should be inward looking considering that each organisation is unique. And different aspects are to be evaluated to shape the cybersecurity culture by looking into organisational cybersecurity maturity level, the security gaps to be fixed (human centre security); existing cultures and values, and the overall cybersecurity threat landscape.

## 5. THE CORE ELEMENTS OF A ROBUST AND EFFECTIVE CYBERSECURITY CULTURE IN CIVIL AVIATION ARE

### 5.1 Leadership

5.1.1 An effective cybersecurity culture depends on the commitment of all in the organisation, starting with executive management taking the lead. Executive Management to provide their full commitment to cybersecurity culture, at all times and across all activities, strategies, policies and organisational objectives.

5.1.2 In that regard, executive management should:

- a. Endeavor to enhance their knowledge of cybersecurity in civil aviation;
- b. abide by cybersecurity rules, processes, and procedures at all times and lead by example;
- c. clearly include cybersecurity as an organisational priority;
- d. enshrine aviation cybersecurity in the written policies of the organisation to become an integral part of the company's management plan;
- e. provide visible support to the implementation of cybersecurity culture;
- f. ensure and support cybersecurity training and capacity building for all personnel;
- g. ensure the processing of cybersecurity reports in a timely fashion and ensure the prompt implementation of any required corrective and preventive actions;
- h. intervene appropriately whenever cybersecurity is compromised; and
- i. monitor the development of the cybersecurity posture of the organisation, cybersecurity culture, and the measures and resources assigned to support the continuous improvement of cybersecurity culture's adoption across the organisation.

### 5.2 Cross-domain links

5.2.1 Consideration towards the multitude of cyber risks and vulnerabilities in every organisation, cross domain links should be formally established.

5.2.2 A multidisciplinary custodian reporting to senior management might be established as a means to support coordination of cybersecurity culture across the organisation.

5.2.3 The custodians' objectives would include the following:

- a. periodically assess the maturity of cybersecurity culture within the organisation;
- b. identify risks and opportunities with regards to cybersecurity culture implementation;
- c. collaboration with different internal stakeholders with regards to cybersecurity culture; and
- d. support the development and implementation of cross-domain activities related to fostering cybersecurity culture in the organisation.

### 5.3 Communication

- 5.3.1 Communication plays an essential role, both internally and externally, in ensuring the implementation of successful cybersecurity culture. It is the main means through which the expected level of awareness can be reached.
- 5.3.2 For communication to be effective, it is reliant on cultivation of certain skills to support a robust cybersecurity culture:
- a. *active listening* – process through which verbal and non-verbal signals are observed, in order to recognize the other individual's values and needs and contribute to the improvement of team communication.
  - b. *adapting communication style to different audiences and situations* – understanding how others communicate and customizing the message in order to better reach them; and
  - c. *clarity of communication* – identify what and how to communicate.
- 5.3.3 Executive Management should ensure that internal policies and guidelines regarding cybersecurity, 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 cybersecurity measures by all staff and helps promote cybersecurity culture in the organisation.
- 5.3.4 In addition, internal communication programmes would greatly assist in:
- a. ensuring that all staff are fully aware of their duties, rights, and the reporting mechanisms in place in the organisation; and
  - b. promoting the organisational digital code of conduct, that includes the processes, measures and controls that staff should comply with at all times.

#### **5.4 Awareness, training and education**

- 5.4.1 Awareness, training and education are key areas of the learning process that should be leveraged for a robust cybersecurity culture. Awareness provides people with knowledge, training teaches skills, and education provides knowledge and skills within a theoretical framework, hence integrating awareness and training.
- 5.4.2 All civil aviation staff who interact with the organisation's digital assets, regardless of their roles or functions, should undertake a cybersecurity awareness, training, and education programme to ensure that they are equipped with required knowledge and skills on aviation cybersecurity risks, measures, and objectives. These programmes should be adapted to the audience, as necessary and possible.
- 5.4.3 Cybersecurity awareness programmes should be delivered to all staff upon their hiring, as well as a recurrent training. The time intervals for the recurrence of the awareness programme should be identified based on the level of maturity of cybersecurity culture in the organisation and can be revisited in line with the development of this maturity level.
- 5.4.4 It is recommended that cybersecurity awareness programmes be delivered at least once in person (in a physical or virtual classroom setting). Cybersecurity is not a familiar topic to all staff and is sometimes hard to be digested without guidance from a professional. As such, interaction with a professional in a classroom setting facilitates the understanding of cybersecurity topics. It allows the trainer to explain concepts, processes, procedures, and controls in a simplified manner to be understood by the non-technically savvy personnel, as well as explain the

benefits in enhancing the cybersecurity posture of the organisation and its positive impact on the overall productivity of personnel.

- 5.4.5 Following an initial in-person awareness/training session, organisations may consider using e-learning methods (computer managed learning) for recurrent training. Such decision should consider the development of cybersecurity culture in the organisation, as well as changes in cybersecurity processes, controls, and procedures introduced in the organisation in response to the evolving cybersecurity risk landscape.
- 5.4.6 Cybersecurity awareness programmes should be delivered by professionals that possess the required technical knowledge. However, one of the challenges faced with technical awareness programmes is the lack of soft skills by the presenters, whereby adequate communication and “sales” skills go a long way in engaging staff and ensuring their buy-in and support to cybersecurity culture. Accordingly, organisations should ensure that awareness programme leaders are equally equipped with the technical knowledge and soft skills necessary to instil in staff behavioural changes to support the adoption of cybersecurity culture.
- 5.4.7 A typical cybersecurity awareness programme should include the following subjects:
- a. the purpose of the awareness programme.
  - b. existing communication mechanisms in the organisation.
  - c. a general overview of cyber risks and events to civil aviation and potential consequences (including examples).
  - d. cybersecurity controls, processes, and procedures of the organisation.
  - e. the role of the human element in safeguarding the organisation against cyber risks.
  - f. the importance of staff reminding each other of organisational cybersecurity principles when observing non-compliant actions by their colleagues.
  - g. overview of the different exploit methods that may target people and their consequences (including examples).
  - h. how to identify suspicious cyber activities.
  - i. the impact of complacency on the organisation (including examples).
  - j. principles of cyber hygiene.
  - k. proper handling of sensitive data and information; and
  - l. reporting mechanisms, how to use them, and follow-up mechanisms.
- 5.4.8 Cybersecurity awareness campaigns should also be used periodically, as a reminder, to reinforce the knowledge and skills of personnel. Various tools are available for that purpose including:
- a. *paper-based tools* – such as posters, brochures, booklets, etc. This type of media can be easily distributed and digested. However, they are passive tools and require frequent update (and a new print with each update).
  - b. *online tools* – such as e-mails, newsletters, messages on screen savers, intranet, short videos, FAQ pages, e-learning (computer managed learning), etc. The main advantage of these tools compared to paper-based tools is their ability to reach the whole organisation. They are relatively easy to update in terms of resources as well as production cost.

## 5.5 Reporting systems

- 5.5.1 A cornerstone of cybersecurity culture is the development and implementation of an internal cybersecurity reporting system. Such system allows the organisation to pro-actively manage its cyber risks, measure the development of the organisation's cybersecurity posture, identify and plan awareness and training needs of staff, and adapt its internal processes, controls, and measures in line with the development of cybersecurity trends and with the maturity of cybersecurity culture.
- 5.5.2 Cybersecurity reporting systems gather elements from both aviation safety and aviation security reporting systems. As such, they address two areas: The first area is reporting of self-actions/errors that are not in line with the organisational information security policies and processes, and the second area is reporting of suspicious/erroneous behaviour of other employees.
- 5.5.3 When developing their cybersecurity reporting mechanism, organisations are encouraged to benefit from the experience gained in developing and implementing aviation safety and aviation security reporting systems.
- 5.5.4 The following elements should be considered when implementing a cybersecurity reporting system:
- a. confidentiality of personal information, whereby personal data is not collected and/or stored. When personal data is collected it should only be used to either gain clarification, further information about the reported occurrence or offer feedback to the reporter.
  - b. to ensure the confidentiality of personal information, a policy should be developed that clearly identifies, and holds accountable, the person(s) tasked with managing, maintaining, guaranteeing the confidentiality, analysing, and following up on collected information.
  - c. providing adequate training to all staff on how to use the reporting system.
  - d. implementing a just culture in cybersecurity reporting, and providing adequate awareness to all staff on how a just culture works so that they are more comfortable providing information; and
  - e. implementing, as applicable, an incentive programme aimed at encouraging staff to report their own errors as well as any suspicious cyber behaviours they observe.

## 5.6 Just culture

- 5.6.1 Organisations should encourage their staff to report cybersecurity incidents through the adoption of a just culture. Just culture is a concept implemented in safety reporting which could be of great value in promoting a cybersecurity culture.
- 5.6.2 In a cybersecurity reporting context, a just culture encourages all staff to report cybersecurity incidents and errors. It is an environment where everyone understands that they will be treated fairly based on their actions rather than the outcome of their actions. In a just culture environment, all staff clearly understand that it is not fair to punish all errors regardless of their circumstances, while at the same time they also understand that it is unacceptable to provide a blanket immunity from punishment as some actions could have malicious intent or could be the result of pure negligence and/or nonchalance. As such, it is important to draw the line between acceptable and unacceptable actions when designing a just culture.

- 5.6.3 A just culture not only defines the responsibilities of staff towards their organisations, but also those of management towards personnel. Those responsibilities should be included in a policy in which the organisation's senior management should:
- a. encourage staff to practice cyber hygiene and commit to recognize their efforts in supporting the organisation in managing cyber risks.
  - b. commit to provide all staff with the adequate cybersecurity procedures, awareness, training, and education to support them in performing their duties.
  - c. assume responsibility if any incident is caused by lack of awareness or promptness in addressing a certain cyber risk; and
  - d. encourage staff to report cyber incidents, hazards, errors, or any suspicious behaviour they witness without fear of reprisal.

## 5.7 Quality control

- 5.7.1 Organisations should implement quality control programmes designed to monitor the effective implementation of cybersecurity measures. Quality control programmes can be an effective tool in keeping staff alert and committed to cybersecurity culture principles. The frequency and rigidity with which quality controls are carried out may have a positive influence on staff by demonstrating management's commitment to cybersecurity objectives and compliance.
- 5.7.2 Regular quality controls of the reporting mechanisms in place should be carried out as part of the quality control programmes.




## 5.8 Continuous review and improvement

- 5.8.1 Organisations should develop a performance indicator framework designed to assess the impact of measures in place on cybersecurity culture as well as to determine the gap existing between desired and actual culture outcomes.
- 5.8.2 As some elements of cybersecurity culture may not be directly observed, a range of possible indicators can be used to measure the effectiveness of cybersecurity culture. Such measures may include:
- a. statistics on reported incidents (considered comparatively with data mined from the organisation's logs) to measure cybersecurity performance of personnel, their level of awareness, and the progress achieved in promoting cybersecurity reporting.
  - b. results of recurrent training sessions.
  - c. results from simulations of malicious attacks to test response of personnel; and
  - d. questionnaires and interviews.

## 5.9 Positive work environment

- 5.9.1 A general positive work environment may also greatly influence commitment of staff to cybersecurity culture and enhance cybersecurity performance.
- 5.9.2 A positive work environment should include, at a minimum:

- a. the involvement of staff in decision-making processes (e.g., suggestions for improvement to cybersecurity awareness training programmes).
- b. the allocation of sufficient time for staff to complete training on proper cyber hygiene.
- c. a mechanism for recognizing good performance (i.e., incentives and/or reward programmes).
- d. the provision of feedback to staff on suggestions and on cybersecurity reports.
- e. setting clear, achievable, and measurable goals with regards to cybersecurity incidents, and periodic feedback to staff on how the organisation is advancing in that regards.
- f. the provision of the necessary procedures, awareness, training, and tools to enable staff to perform their duties; and
- g. providing staff with the appropriate levels of autonomy and responsibility.

<b>DEVELOPED BY:</b>		
	<b>DIKELEDI MZIMBA</b>	<b>28 MARCH 2022</b>
<b>SIGNATURE OF AVSEC RS</b>	<b>NAME IN BLOCK LETTERS</b>	<b>DATE</b>
<b>REVIEWED &amp; VALIDATED BY:</b>		
	<b>MARCHE' ARNOLD</b>	<b>28 MARCH 2022</b>
<b>SIGNATURE OF ACTING M: OS</b>	<b>NAME IN BLOCK LETTERS</b>	<b>DATE</b>
<b>APPROVED BY:</b>		
	<b>LUVUYO LULAMA GQEKE</b>	<b>28 MARCH 2022</b>
<b>SIGNATURE OF E: AVSEC</b>	<b>NAME IN BLOCK LETTERS</b>	<b>DATE</b>