Air Traffic Management Cybersecurity Policy Template Checklist

Introduction

The present document is a checklist that aimed a self-assessing of all the requirements on cybersecurity implementation explained in the Air Traffic Management Cybersecurity Police Template.

The Document is not a mandatory requirement for implementation, but it contains relevant information that will support the development of your own Cybersecurity Policy Manual.

Scope

This document covers the whole aviation functional structure and all aviation stakeholders such as Civil Aviation Authorities, Air Navigation Service Providers and any entity or organization that is part of the State Aviation System to ensure the implementation of cybersecurity procedures and methods in all services under the State oversight such as:

- ✓ Air Traffic Services Units (Aerodrome control tower or aerodrome control – TWR, approach control service - APP and Area control centre -ACC)
- ✓ Communication, Navigation and Surveillance (CNS) data and infrastructure
- ✓ Digital information systems (aeronautical information, meteorological information and other supporting decision-making information)
- ✓ Systems for aviation interoperability
- ✓ Others according with State services and operations

This document applies to the whole aviation system locations and premises hosting:

- ✓ Information required by Air traffic management (ATM) services
- ✓ Information technology (IT) infrastructure that ATM services rely on
- ✓ Operational technology (OT) and Interconnected Industrial and Automated Controlled Systems (IACS)
- ✓ Extended services and partnership, and related information system interconnections
- ✓ All aviation personnel and external organizations having access to air navigation information, services and facilities

In cooperation with

ICAO canso AIRBUS

Air Traffic Management Cybersecurity Policy Template Checklist

State:
Point Of Contact (s): Please Introduce Name, e-mail and telephone number of each person designate by the State.

CYBERSECURITY CHECKLIST

1. ATM Security Documentation

-> ATM CYBERSECURITY POLICY TEMPLATE, CHAPTER 6

		Yes	In Progress %	No
1.1	Have you established an Information Security policy for your organization?			
1.2	Have you set up ISMS for your organization?			
1.3	Is your ATM documentation: • Implemented? • And maintained? • Based on a risk management approach?			
	Have you identified and scoped your infrastructure (e.g. as "IT", "OT", and "IACS") so its security can be appropriately and proportionately managed?			

IT Infrastructure	OT and IACS Infrastructure

	Attach other sheets if necessary, to list all IT, OT and IACS infrastructure

Air Traffic Management Cybersecurity Policy Template Checklist

2. Risk Management -> ATM Cybersecurity Policy Template, Chapter 7				
		Yes	**In progress %**	**No**
2.1	Is security addressed in all phases of the system life cycle?			
2.2	Do you have a defined and repeatable risk management procedure (methodology) in place?			
2.3	Are security risks: • tracked? • monitored? • periodically reviewed?			
		Yes	**In progress %**	**No**
2.4	Have you taken steps to process vulnerability management on systems?			
2.5	Have you identified all ATM assets (data, systems, personnel...) and established control procedures for them?			
2.6	Have you empowered the right personnel for making treatment decisions on Security risks?			
2.7	Do you have Information Security Management processes defined? (addressing all security activities)			
2.8	Do you have established technical security measures and operational security measures (policies and processes)? The intention of this is to reduce risk to an acceptable level regarding to human error, Accident or incident, Impact from natural disaster and others.			
2.9	Do you have identified interfaces to ensure efficient and coordinated treatment of security risk about ATM security?			
2.10	Have you established a risk management process covering ATM information security risks, with regular review and monitoring?			
3. Security Governance and Organization -> ATM Cybersecurity Policy Template, Chapter 8				
		Yes	**In progress %**	**No**
3.1	Have you established an appropriate authority for ATM security management at a Unit level?			

Air Traffic Management Cybersecurity Policy Template Checklist

3.2	Have you established roles and responsibilities within ATM security risk management?			
3.3	Have you implemented defined processes for threat intelligence and monitoring			
3.4	Have you implemented defined processes for incident and crisis management?			
4. Human Resources (Security measures during all employment phases) -> ATM Cybersecurity Policy Template, Chapter 9				
		Yes	**In progress %**	**No**
4.1	Before employment: do you use measures such as background checks in accordance with local regulations?			
4.2	During employment: do you develop a security culture through regular training and raising awareness?			
4.3	After employment: do you protect yourself by ensuring the de-provisioning process for access, and by reminding staff of nondisclosure commitments (where allowed by law)?			
4.4	Do you have procedures to assign and limit staff access according to their responsibilities?			
5. Asset Management -> ATM Cybersecurity Policy Template, Chapter 10				
		Yes	**In progress %**	**No**
5.1	Have you taken an inventory of ATM assets and kept it up to date?			
5.2	Does the inventory include criticality evaluation (regarding safety and operability) for each asset?			
5.3	Have you considered logical and physical access, and made sure there is consistency between them?			
		Yes	**In progress %**	**No**
5.4	Is all ATM data considered and classified, and protected to an adequate level?			
5.5	Do you have procedures to ensure that all ATM data will be protected during storage, processing and exchange, in line with its sensitivity profile?			
6. Access Control -> ATM Cybersecurity Policy Template, Chapter 11				
		Yes	**In progress %**	**No**
6.1	Is all access to ATM assets through a suitable access			

	verification process, to avoid unacceptable risk?			
6.2	Do you have controls covering physical and logical access to systems?			
7. Physical and Environmental Security of CNS/ATM Components -> ATM CYBERSECURITY POLICY TEMPLATE, CHAPTER 12				
		Yes	**In progress %**	**No**
7.1	Have you ensured that ATM physical security safeguards IT, OT, IACS and CNS/ATM infrastructure against unlawful interference and unauthorized access?			
7.2	Have you ensured that ATM physical security identifies zones hosting CNS/ATM assets according to their criticality (from safety and operability perspectives)?			
7.3	Have you implemented ATM physical security measures to protect all CNS/ATM from unlawful or intentional interruption of services and operations?			
7.4	Have you implemented ATM physical security to protect incoming and outgoing information flows between storage zones and data centres?			
8. Operations Security -> ATM CYBERSECURITY POLICY TEMPLATE, CHAPTER 13				
		Yes	**In progress %**	**No**
8.1	Have you established trust zones?			
8.2	Have you established procedures to ensure ATM cybersecurity coordination of security operations, monitoring and continuous improvement of information processing?			
8.3	Have you ensured that ATM cybersecurity operations include IT, OT, IACS and CNS/ATMs infrastructure in the scope of security operations?			
8.4	Have you implemented ATM cybersecurity operations to maintain the effectiveness of security measures throughout their lifecycle?			
8.5	Have you established a security perimeter through ATM cybersecurity zones for physical and logical zones?			
		Yes	**In progress %**	**No**
8.6	Do you have procedures to prevent the exploitation of technical vulnerabilities on IT, OT, IACS and			

Air Traffic Management Cybersecurity Policy Template Checklist

	CNS/ATM infrastructure?			
8.7	Do you have security controls around the use of personal mobile devices for CNS/ATM activities (e.g. is their use forbidden)?			
8.8	Do you take steps to ensure that personal mobile devices do not represent a risk for the security of CNS/ATM activities (e.g. plugging in a personal device to operational equipment to charge)?			

9. Communications Security

-> ATM Cybersecurity Policy Template, Chapter 14

		Yes	In progress %	No
9.1	Do you collect and maintain an up-to-date mapping of networks and their interconnections?			
9.2	Do you ensure ATM networks are logically or physically segregated based on their criticality regarding safety and operability?			
9.3	Do you take steps to ensure that wireless technologies and access to the Internet do not constitute an unacceptable risk to safety and security?			

10. System Acquisition, Development and Maintenance

-> ATM Cybersecurity Policy Template, Chapter 15

		Yes	In progress %	No
10.1	Is information security is an integral part of your management of CNS/ATM information systems throughout the entire lifecycle?			
10.2	Do you ensure that your CNS/ATM information systems are designed based on the following principles: • No single, nor common point of vulnerability? • Defined and verified use of security coding rules? • Vulnerability management on COTS software and hardware? • The use of appropriate industry standards and recommendations (e.g. NIST, OWASP, EUROCAE/RTCA, etc.)?			

Air Traffic Management Cybersecurity Policy Template Checklist

11. Suppliers and Partners Relationships -> ATM Cybersecurity Policy Template, Chapter 16				
		Yes	**In progress %**	**No**
11.1	Do you evaluate the security maturity of suppliers and partners prior to contract?			
11.2	Does your risk management process also address risk on suppliers?			
12. Security Incident Management -> ATM Cybersecurity Policy Template, Chapter 17				
		Yes	**In progress %**	**No**
12.1	Do you have communication procedure and communication lists in case of security incident or weakness identification?			
13. Security Aspects of Business Continuity Management -> ATM Cybersecurity Policy Template, Chapter 18				
		Yes	**In progress %**	**No**
13.1	Do you have defined interfaces between ATM business continuity and risk management processes?			
13.2	Do you perform crisis management exercise and test based on ATM security case?.			
14. Protection of Personal Data -> ATM Cybersecurity Policy Template, Chapter 19				
		Yes	**In progress %**	**No**
14.1	Do you have defined interface between DPO and ATM security process?			
15. Compliance -> ATM Cybersecurity Policy Template, Chapter 20				
		Yes	**In progress %**	**No**
15.1	Do you perform regular Third party Security audit of ATM/CNS information systems?			
15.2	Do Security Results Trigger Risk Assessment Updates?			

- END -