Classification: Public use
Version: 3.0
Date: 2023-02-20

Annex No 5

APPROVED BY THE DECISION OF THE BOARD OF DIRECTORS

NO. 2023/03/07-1 ON 7 MARCH 2023

Information Security Policy

Contents

1. Introduction

Information Security Policy (the Policy) is a high-level security control document which sets out the key requirements and guidelines regarding information security of Avia Solutions Group (ASG) PLC and its subsidiary companies. Information security refers to the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, personal and sensitive information or data controlled and processed by Avia Solutions Group (ASG) PLC from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption. The Policy establishes the scope of required policies and procedures set due to information availability, integrity, and confidentiality, common know as CIA Triade. Compliance with the Policy shall ensure prevention of information security incidents, including, but not limited to, data breaches, security, or cyber security incidents in Avia Solutions Group (ASG) PLC and its subsidiary companies.

2. Purpose

The main purpose of the Policy is to preserve information security of Avia Solutions Group (ASG) PLC and its subsidiary companies and define information security rules and guidelines that all employees, third parties, vendors, their employees and representatives or other parties shall comply when using information of Avia Solutions Group (ASG) PLC and its subsidiary companies, such as, but not limited to, information systems and/or assets, networks, other types of data or its access. The Policy includes the risk management of information leakage due to finance, reputation, legal risk by complying regulatory requirements, security standards and best information security worldwide practices for ensuring confidentiality, integrity, and availability of information.

This Policy is not limited to, but is guided by:

- ISO/IEC 27001&27002
- The General Data Protection Regulation (EU) 2016/679 (GDPR)
- The European Union Agency for Cybersecurity (ENISA) standards
- NIST Cybersecurity framework
- Center for Internet Security Critical Security Controls

3. Scope

The Policy applies to all Avia Solutions Group (ASG) PLC and its subsidiary companies' employees and staff, third parties, vendors, their employees and representatives or other parties of Avia Solutions Group (ASG) PLC and its subsidiary companies. From the technical perspective the Policy applies, but not limited to:

- IT networks and network devices
- IT assets
- Information systems

- IT Services
- Hardware or software
- Data processing process
- BYOD devices
- IOT devices

To define scope within the rest of the policy, the following abbreviations are used:

Abbreviation	Meaning
ASG	Avia Solution Group (ASG) PLC. Dariaus ir Gireno st. 21a, LT-02189 Vilnius, Lithuania.
ASG CEO	ASG Chief Executive Officer
ASG group	ASG with ASG subsidiary (-ies)
Company (-ies)	ASG subsidiary (-ies)
Head of Cyber Security (CISO)	ASG Head of Cyber Security (CISO)
Head of IT Operations	ASG Head of IT Operations

4. Responsibilities

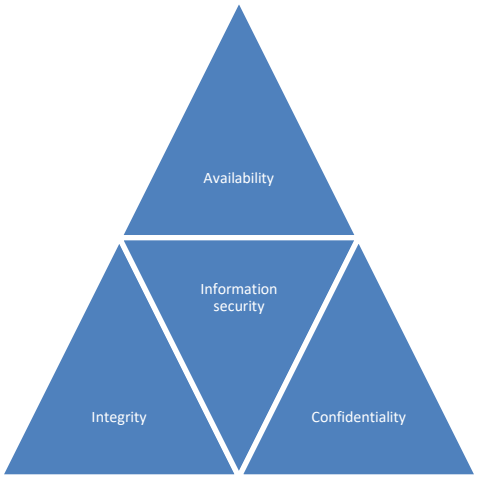
- Head of Cyber Security (CISO)
  - implementation of the Policy in ASG Group
  - organization of internal audits of organization
  - Information security training program
- Executive of the companies are responsible for:
  - ensuring adaptation, implementation and of the Policy in the managed companies
  - familiarization of employees with information security policy
- Information owner responsible for
  - ensuring and adopting the Policy requirements to controlled IT environment
- IT managers are responsible for
  - implementation of the Policy requirements in controlled environment from technical perspective
- All employees are responsible for:
  - Compliance with information security policy

- Data classification by information classification rules

- Human Resources are responsible for acknowledging each new employee with the relevant ASG Group IT and Security Policies upon the first day of commencing work with ASG Group.

5. Definitions

- **Confidentiality** – designed to prevent sensitive information from unauthorized access attempts. It is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes. Common principle "need-to-know" is implemented.
- **Integrity** – the consistency, accuracy, and trustworthiness of data over its entire lifecycle. Data cannot be changed in transit and altered by unauthorized people. It consists of maintaining and assuring the accuracy and completeness of data over its entire lifecycle. It is information security principle that involves human/social, process, and commercial integrity, as well as data integrity by conducting credibility, consistency, truthfulness, completeness, accuracy, timeliness, and assurance.
- **Availability** – information should be consistently and readily accessible for authorized parties. It consists of hardware or software, technical infrastructure and information systems, database, assets and information in any type of data storage. Basic principle- information must be available when it is needed, for authorized person only.
- **Information Owner** – employee which creates, develop, specify, or prepare any data and responsible for such data classification, processing, access, dissemination and disposal.
- **CIA** – model which consists of information security principles ensuring the Confidentiality, Integrity, and Availability of information.



6. Enforcement

The failure to comply with this Policy is a serious violation. Any employee found to have violated this Policy may be subject to disciplinary action.

7. Policy

The Information Security Policy is an information security standard of ASG Group. This standard defines the scope of additional policies that make up the overall scope of information security. Information Security Policy is applicable in line with internal data protection regulations in ASG Group (ex. Personal data processing policy, Data storage policy, Procedure for managing personal data breaches etc.). Information security guidelines, rules or any other control is provided in separate information security policies which must be acceptable to use in ASG Group.

7.1. Information Security Policy

A high-level security control document which sets out the key requirements and guidelines regarding information security of ASG Group by establishing policies that make up the overall scope of information security as listed below.

7.2 Security Governance

Security Management must be designed and maintained through a coherent set of policies, processes, and systems to manage risks to its information assets, thus ensuring acceptable levels of information security risk.

7.3 Human Resource Security

The contractual agreements with employees and contractors must state theirs and the ASG Group's responsibilities for Information Security.
All staff must undertake security training relevant to their job function. Training must be conducted on an annual basis, or more frequently, as required to address human error, theft, fraud, and other related security risks.

7.4 Asset Management

Set of objectives and guidelines for establishing requirements to identify, classify and register IT assets issued to the end-user or business needs must be implemented. The process and required documentation for asset management consists of assets naming convention, replacement strategy, standards for equipment, equipment usage period and maintenance.

7.4.1 Acceptable Use

Set of requirements and guidelines regarding to information usage of ASG Group (physical or virtual) must be designed. The Acceptable Use Policy describes rules that shall be followed processing any data, including IT resources management.

7.4.2 Information Classification and Labeling

Set of information classification and management guidelines to ensure that sensitive information is handled well with appropriate procedures and marking must be implemented. ASG Group data, information, media, and assets must be handled in accordance with their classification.

7.5 Access Management

Set of requirements for authorization of users or devices to disallow unauthorized access to the information (the principles of *need to know* and *least privilege*) shall be designed. Access control management consists of requirements and guidelines for physical and virtual access to information, data, physical devices, and offices. The required documentation and process establishes security controls how the information of ASG Group shall be protected via control of access, so it is not improperly disclosed, modified, deleted, altered, or rendered unavailable.

7.5.1 Authentication Methods

Set of rules to enhance IT security by encouraging end users and privileged users to use strong and complexify passwords and use them properly. It consists of password strength, change, or store requirements. The stronger authentication methods (such as multi-factor authentication) based on the identified risk must be implemented.

7.6 Cryptography Management

Encryption Key lifecycle shall be implemented to protect data and communication.

7.7 Physical and Environmental Security

Physical security measures must be defined and implemented to protect premises, data centers and other areas from unauthorized access. Authorization must be assigned in accordance with the employee's tasks and responsibilities.

7.7.1 Clean Desk (Desktop)

Set of requirements of workplace (physical or virtual) for secure day-to-day work following basic and standard security practices must be designed and implemented. The Clean Desk Policy consists of rules of general access, information sharing and publicity due to the human factor, both work hours and after working hours.

7.8 IT Operational Security

The ASG Group must ensure that only security tested and approved systems are deployed into the Prod environment.

7.8.1 Change Management

All changes to the applications, information systems and network components must be registered, assessed, tested, approved, and implemented using a Change Management Process.

7.8.2 Security Monitoring

Set of requirements and guidelines, how the information is integrated in security systems, for security monitoring (detection), monitoring and alerting uses cases to appropriate channels and stakeholders shall be implemented. The process and required policies include organization and technical aptitude for CIA in security monitoring perspective.

7.8.3 Backup Management

The backup management indicates security requirements for backing up, storing, and destroying backup data. All employees should enable automatic backups of systems and information and adopt practices of creating backups of important documents.

7.8.4 Malware Protection

Malware protection tools and antivirus solutions should be deployed on all workstations. Access to malware protection configuration must be restricted to privileged users. Network traffic, emails, and data transfer from third party service providers must be scanned before uploading to the internal ASG Group network.

7.8.5 Vulnerability and Patch Management

Set of patch management requirements, including patching and vulnerability scanning process used to update the software, operating systems, applications, or other IT device must be implemented. The process indicates how to discover vulnerabilities on assets, network, or any IT target. Vulnerability and Patch Management documentation sets out remediation times by categorization of risk, priority and security requirements regarding to the possible risk for cyber-attacks and CIA disruption.

7.8.6 System Hardening

Set of operating system hardening guidelines from technical and operational perspective shall be designed. System hardening is advanced security measure to secure a business due to operating system, applications or other any IT device for secure and trusted functionality, regarding to business continuity and IT risks.

7.8.7 Penetration Testing

Set of requirements and classification for a penetration test shall be designed. The penetration testing process indicates penetration testing methodology, requirement for penetrations testers, penetration testing schedules, including scope.

7.9 Communication Security

Networks must be segmented to protect IT assets. Set of requirements and guidelines how personal devices (BYOD), which are used for managing information of ASG Group, shall be configured and secured.

7.9.1 Encryption

Set of requirements and guidelines how information and information assets shall be encrypted, by following secure and approved algorithms, technologies, and decryption keys storage shall be designed.

7.9.2 Remote Access

Set of requirements and guidelines for remote access to information from external networks, reaching resources globally and ensuring CIA shall be implemented.

7.9.3. Wi-Fi Management

Set of requirements and guidelines how Wi-Fi networks must be managed in secure perspective shall be designed. The requirements include rules for authorization, information sharing in internal and external networks, monitoring, and ensuring CIA, also standard Wi-fi equipment hardening guidelines.

7.10 Secure Development

Develop business applications and information systems in accordance with an approved system development lifecycle, which includes applying industry good practice and incorporating information security during each stage of the lifecycle.
The requirements include but are not limited to full production system exposing to internet, testing and maintenance.

7.11 Supplier Management

Set of third-party risk management requirements, for secure information processing for non-ASG Group employees shall be designed. It includes access rights and privileges to information granting and third parties end-user equipment requirement from security perspective.
Processes, Procedures, and other supporting information must be documented detailing controls to be implemented to mitigate risks related with suppliers or other third-party service providers.

7.12 Security Incident Management

An information security incident management framework must be established. The framework should include relevant individuals and tools required by the information security incident management, escalation and analysis processes for cyber security incidents investigation and incident response of any cyber-attack. It includes responsibilities, plan, tools, and playbooks to efficiency in business continuity due to the security incident.

7.12.1 Log Management

Set of requirements and guidelines of event logging, due to the business efficiency troubleshooting, or cyber incident analysis and evidence collection shall be established. Log management process include, but is not limited to, logging technologies, scope, and retention.

7.13 Business Continuity and Disaster Recovery Management

Business continuity and disaster recovery strategy defines how a particular Company responds to disruptive events, such as cyber-attacks, natural disasters, and power outages. Any employee involved in procedures for reporting incidents, implementing the disaster recovery plan, and escalating appropriate response to a disaster must be formally acknowledged with the disaster recovery plan. Disaster recovery and business continuity plans for critical business functions, supporting processes and information assets, must be tested at least annually.

7.14 Compliance Management

The ASG Group must ensure that information security controls are implemented, consistently prioritized, and addressed according to information security obligations associated with legislation, regulations, contracts, industry standards and ASG Group policies.
The ASG Group must ensure that security controls have been implemented effectively, that risk is being adequately managed and to provide the owners of target environments and executive management with an independent assessment of their security status.

8. Exceptions

Exceptions to the guiding principles in the Policy must be documented and formally approved by the Head of IT Operations and Head of Cyber Security. Exception requestor must provide a reasonable explanation for why the policy exception is required and risks created by the policy exception.

9. Provision

All changes and revisions are made by the Head of Cyber Security on an annual basis or as needed.

10. Approval History

Version	Approval date	Approved By	Comments

11. Version History

Version	Date	Edited By	Reason/Comments
1.0	2021.10.01	Tautvydas Jasinskas	Initial draft.
2.0	2022.06.15	Tautvydas Jasinskas	Document updated.
3.0	2023.02.20	Audrone Gailiute	Document alignment with ISO 27001 standard.