Policy Name:	Product and Service Cybersecurity Policy		
Release Date:	June 2025	Version:	1.2
Released by:	Center of Excellence, Automotive \ Product Security	Applies to:	Everyone

Between

Harman International
400 Atlantic Street, I5th Floor
Stamford, CT 0690I USA

- hereinafter referred to as “HARMAN” -

and

and the Supplier

- HARMAN and Supplier hereinafter collectively referred to as the “Parties” -

Table of Contents

I. Purpose 3
II. Scope 3
III. Terms & Definitions 3
IV. Framework 4
1. Basic Cybersecurity Requirements 4
2. Access to Network and Information Systems 6
3. Provision of Cloud Computing Services or Data Center Services for HARMAN 8
4. Supply of Software or other Products with Digital Elements 9
V. Annex I: Supplier Incident Notification Contact Details 15
VI. Annex II: HARMAN Incident Notification Contact Details 16
VII. Approval and Ownership 17
VIII. Revision History 17

I. Purpose

As a result of new European Union legislation on cybersecurity, HARMAN is and will be subject to a large number of new cybersecurity requirements, in particular for the manufacturing of products with digital elements and radio equipment. These requirements are based on existing and evolving legal acts and frameworks, including but not limited to the Cyber Resilience Act, the NIS-2 Directive, and the Radio Equipment Directive. HARMAN's obligations also include the requirement to comply with the relevant legal acts throughout the supply chain.

II. Scope

This Supplier Cybersecurity Framework ("**Framework**") serves as the basis for all cybersecurity requirements to be met by the Supplier and, unless expressly contractually agreed otherwise, takes precedence over all other contractual agreements.

III. Terms & Definitions

(1) **Cloud Computing Service:** A digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations.

(2) **Coordinated Vulnerability Disclosure (CVD):** A structured process for the responsible identification, reporting, and remediation of security vulnerabilities.

(3) **Data Centre Service:** A service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of IT and network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control.

(4) **Framework**: This Supplier Cybersecurity Framework that outlines the cybersecurity requirements and standards to be met by the Supplier.

(5) **Hardware Bill of Materials (HBOM):** A detailed inventory of all hardware components, assemblies, and subassemblies that make up a physical product or system. The HBOM provides visibility into the product's hardware composition, including manufacturer details, part numbers, firmware versions, and dependencies.

(6) **Incident:** As defined in Article 6, point (6), of Directive (EU) 2022/2555 (NIS-2 Directive): An event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems.

(7) **Network and Information System**: As defined in Article 6, point (1), of Directive (EU) 2022/2555 (NIS-2 Directive). For the purposes of this agreement, this term explicitly includes both Information Technology (IT) systems and Operational Technology (OT) systems used for managing industrial, operational, or automated processes.

(8) **Product with digital elements**: A software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately.

(9) **Provided Products and Services:** The provided products and services include all products and services supplied by the Supplier to HARMAN, regardless of whether they involve the provision of hardware, software, IT systems, operational services, or any other type of deliverable. This includes both tangible and intangible products, as well as any associated support, maintenance, and cybersecurity measures.

(10) **Radio equipment**: An electrical or electronic product, which intentionally emits and/or receives radio waves for the purpose of radio communication and/or radiodetermination, or an electrical or electronic product which must be completed with an accessory, such as antenna, so as to intentionally emit and/or receive radio waves for the purpose of radio communication and/or radiodetermination.

(11) **Radio Equipment Directive (2014/53/EU) (RED)**: A European Union directive that establishes regulatory requirements for the placement of radio equipment on the market.

(12) **Risk:** The potential for losses or disruptions caused by a security incident affecting the availability, integrity, authenticity, or confidentiality of network and information systems.

(13) **Service Level Agreement (SLA)**: A formal agreement between HARMAN and the Supplier that defines the measurable service performance criteria, responsibilities, and expectations for the Supplier's services. The SLA outlines specific metrics such as availability, response times, and support levels to ensure that the Supplier meets agreed-upon standards.

(14) **Software Bill of Materials (SBOM)**: A detailed inventory of all components, libraries, and dependencies within a software application or system. The SBOM provides visibility into the software's composition, including open-source and third-party elements, to help identify potential vulnerabilities and maintain compliance with security standards.

(15) **Supplier**: Any entity or individual that provides goods, services, or solutions to HARMAN under the terms of a contractual agreement.

(16) **Testing**: Comprehensive evaluations and examinations conducted by HARMAN to identify vulnerabilities, malicious code, and other security-related risks in the provided services.

IV. FRAMEWORK

1. Basic Cybersecurity Requirements

a) Risk Management

(1) The Supplier undertakes to take appropriate and proportionate technical, operational and organizational measures to manage the risks posed to the security of network and

information systems it uses for the provision of its services and to prevent the impact of incidents on HARMAN.

(2) The measures shall ensure a level of security of network and information systems appropriate to the risks posed, comply with the state-of-the-art and, where applicable, the relevant European and international standards. Additionally, the measures shall incorporate best practices for the hardware and software technologies utilized.

(3) When assessing the adequacy of the measures, the Supplier will comply with and ensure it is following any cybersecurity policies provided by HARMAN, including any updates or changes to these policies throughout the duration of the contract. The applicable cybersecurity policies can be accessed at [https://www.harman.com/supply-chain].

b) Evaluation and Testing of Information Security

(1) The Supplier shall test and evaluate the information security of the provided products and services before they are provided and – in the case of continuing obligations – regularly during the contractual relationship. The Supplier shall document the results in the industry-standard manner and make them available to HARMAN immediately and without delay upon request without restrictions.

(2) HARMAN is entitled, but not obliged, to test and examine the provided products and services comprehensively at any time for vulnerabilities, malicious code and other security-related risks. Such tests may include, but are not limited to, white-box penetration testing and other industry-standard security assessments. The testing may also be carried out by a qualified third party contracted by HARMAN and bound to confidentiality. The Supplier shall grant HARMAN and/or third parties contracted by HARMAN the rights and necessary third-party consent for the testing. The Supplier shall support HARMAN or third parties contracted by HARMAN in conducting the testing upon request and provide any necessary information, including, but not limited to, documents, source code, and any other details required to perform the testing.

c) Incident Management

(1) The Supplier shall designate the persons responsible for ensuring information security and business continuity management in **Annex I** of the relevant Master Agreement or other relevant agreements (eg. SOW, Awards Letter, …) and provide their relevant contact information to HARMAN. The Supplier shall inform HARMAN without delay of any changes to these positions or their contact details.

(2) The Supplier shall immediately notify HARMAN of any potential or actual incident electronically, via email, using the contact details specified by HARMAN in **Annex II**.

(3) In the event of an incident, the Supplier shall – in close coordination with HARMAN and at its own expense – immediately take all necessary steps to clarify the facts and take effective measures which do not impair the provision of the provided services or – if this is impossible – impair them as little as possible.

(4) The Supplier shall without being asked, immediately and continuously

i. inform HARMAN of the results of the investigation of the incident and the measures taken and, upon request, provide HARMAN immediately with all further information and documentation required to fulfill HARMAN's own legal obligations (in particular reporting obligations), and

ii. provide HARMAN with reasonable support in taking the necessary measures to contain and remedy the incident.

d) Control Rights

(1) Upon request, the Supplier shall provide HARMAN immediately with written proof of compliance with the provisions of this Framework, including but not limited to recognized test reports, documented risk assessments and risk-assessment measures taken.

(2) The Supplier grants HARMAN the right to inspect and review the information security management system and all information security measures taken by the Supplier. HARMAN and/or third parties contracted by HARMAN and bound to secrecy may enter the premises of the Supplier during normal business hours for this purpose.

(3) The costs of the inspection shall be borne by the Supplier if breaches of this Framework or the contractual agreements between HARMAN and the Supplier are identified.

e) Subcontractors

The Supplier shall impose comparable obligations, but in no event less stringent than those set forth in this Framework, on any subcontractor that the Supplier uses to perform its contractual obligations to HARMAN. The Supplier shall ensure that these are passed on, monitored and complied with along the whole supply chain.

f) Cybersecurity Standards and Best Practices

The Supplier acknowledges the importance of maintaining strong cybersecurity practices in line with recognized industry standards. Certifications such as, including but not limited to, ISO/IEC 27001, TISAX, or ISO/SAE 21434 can support the implementation of effective security measures and enhance overall resilience. While obtaining such certifications is not a requirement under this Agreement, they may serve as a valuable reference for strengthening cybersecurity capabilities.

2. Access to Network and Information Systems

a) Access Control

(1) If not otherwise specified by HARMAN, the Supplier shall establish, implement, and maintain a comprehensive access control concept to manage and regulate access by its employees, contractors and third parties to HARMAN's network and information systems. This concept shall ensure that access is granted strictly on a need-to-know basis and aligned with each user's role and responsibilities.

(2) The access control concept must include procedures for assigning, reviewing, and revoking access rights, as well as protocols for monitoring and managing privileged access.

(3) The Supplier shall regularly review and update the access control concept to address emerging security risks and ensure compliance with current cybersecurity standards and best practices. All employees with access to critical systems must be made aware of and trained on the concept.

(4) The Supplier shall provide the access control concept to HARMAN immediately upon request.

b) Authentication

(1) The Supplier shall implement robust password policies and authentication mechanisms to ensure secure access to HARMAN's network and information systems.

(2) Password policies must require a high level of complexity and minimum length, as well as regular password updates. Where applicable, multi-factor authentication shall be enforced to further protect access to critical systems and sensitive information. Additionally, the use of hardcoded passwords, secrets, and sensitive details in hardware products shall be limited as much as possible.

(3) Authentication procedures shall be regularly reviewed and updated to maintain security according to the state-of-the-art, taking into account emerging threats and vulnerabilities.

(4) The Supplier shall provide the respective policies to HARMAN immediately upon request.

c) Remote Access

(1) The Supplier shall establish and maintain secure remote management protocols to prevent unauthorized access to HARMAN's network and information systems. Remote access shall only be granted to authorized personnel and shall be strictly limited to essential tasks. The Supplier is further required to ensure that any of its third parties or subcontractors involved in providing services to HARMAN adhere to equivalent security standards. Upon request of HARMAN, the Supplier undertakes to use only the remote access software provided by HARMAN for all remote maintenance work on HARMAN's systems.

(2) The Supplier shall implement logging and monitoring of all remote access sessions to detect and respond to potential incidents. Logs shall be retained for a minimum period of twelve (12) months and shall be reviewed regularly to ensure compliance with security standards.

(3) The Supplier agrees that all remote access sessions may be logged by HARMAN, including the date, time, type of access and purpose of the remote maintenance.

d) Confidentiality

(1) The Supplier shall ensure that all of its employees, contractors, and third parties with access to HARMAN's network and information systems, whether through access

management, remote management or any other means, are bound by strict confidentiality agreements and have completed the necessary training.

(2) The Supplier shall implement measures to prevent unauthorized disclosure of sensitive information, including but not limited to, limiting access to information on a need-to-know basis and utilizing encryption where appropriate.

3. Provision of Cloud Computing Services or Data Center Services for HARMAN

a) Operating Concept for SaaS and other Cloud Services

(1) The Supplier shall establish and maintain an operating concept that includes the following features:

i. use and provision: description of the procedures and requirements for the use of the Supplier's systems and applications;

ii. exit management: description of the procedures for the proper decommissioning of the Supplier's systems and applications at the end of the contract term or at HARMAN's request;

iii. updates: processes for regular updates of the Supplier's systems and applications;

iv. maintenance: description of planned maintenance activities, including schedule, responsibilities and troubleshooting procedures;

v. product responsibility: definition of the Supplier's responsibilities for the security, integrity and performance of its products and services during the term of the contract;

vi. Coordinated Vulnerability Disclosure ("**CVD**"): The Supplier shall adhere to a structured CVD process, ensuring timely identification, assessment, and mitigation of vulnerabilities that may affect the provided products and services.

vii. incident management and reporting: policies and procedures to identify, assess and respond to incidents affecting data center operations;

viii. data backup and recovery concept: description of the strategies, procedures and technologies for backing up and restoring data;

(2) The Supplier undertakes to develop and document the operating concept in accordance with industry standards and to keep it up to date. At HARMAN's request, the Supplier shall make the operating concept available and explain the procedures and guidelines contained therein.

(3) Details of the Supplier's applications are regulated in a Service Level Agreement ("**SLA**").

b) Monitoring and Performance Metrics

(1) The Supplier shall implement continuous monitoring tools and processes to track and maintain data center performance in alignment with the service levels agreed upon in the SLA.

(2) Monitoring metrics shall include, at a minimum, system availability, incident frequency and resolution time, as well as resource utilization. The Supplier shall provide HARMAN with regular performance reports, highlighting any deviations from the agreed service levels and actions taken to restore compliance. The specific monitoring cycle times and reporting intervals shall be defined in the applicable SLA.

c) Physical Security Measures

(1) The Supplier shall implement robust physical security measures at all data center facilities used for the provided services for HARMAN to prevent unauthorized access and protect the integrity of network and information systems.

(2) Physical security controls must include, at a minimum, 24/7 monitoring, secure access points with multi-factor authentication for entry, and video surveillance. All visitors and non-authorized personnel accessing the data center facilities must follow established security protocols, and access must be logged and reviewed regularly.

(3) Details of physical security measures must be regulated in a respective policy.

4. Supply of Software or other Products with Digital Elements

a) Essential Cybersecurity Requirements

(1) The Supplier shall ensure that the product provided will be designed, developed and produced in such a way that the product ensures an appropriate level of cybersecurity based on the identified risks of the product provided.

(2) The Supplier shall ensure that the product provided fulfills, as applicable, at least the following essential cybersecurity requirements:

i. The product will be made available on the market without known exploitable vulnerabilities in relation to the product provided.

ii. The product will be made available with a secure by default configuration, unless otherwise agreed, including the possibility to reset the product to its original state.

iii. Protection of the product from unauthorized access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorized access.

iv. Protection of the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks.

v. Minimizing the negative impact of the product itself or connected devices on the availability of services provided by other devices or networks.

vi. Limitation of attack surfaces, including external interfaces.

vii. Reduction of the impact of an incident using appropriate exploitation mitigation mechanisms and techniques.

viii. Protection of the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state-of-the-art mechanisms, and by using other technical means.

ix. Protection of the integrity of stored, transmitted or otherwise processed data (personal or other), commands, programs and configuration against any manipulation or modification not authorized by the user, and report on corruptions.

x. Processing only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product provided (minimization of data).

xi. Providing the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.

(3) The Supplier shall ensure that any components sourced from third parties comply, at a minimum, with the same cybersecurity requirements that the Supplier is obligated to meet under this Agreement. The Supplier shall further ensure that such components do not compromise the cybersecurity of any product provided.

(4) The Supplier may maintain public software archives enhancing access to historical versions. In those cases, HARMAN shall be clearly informed in an easily accessible manner about risks associated with using unsupported software.

(5) The Supplier shall ensure that appropriate procedures are in place to maintain the conformity of the provided product with cybersecurity requirements throughout the entire production series. The Supplier shall take into account any changes in the development and production process, as well as modifications to the design or characteristics of the product. Furthermore, the Supplier shall consider changes to harmonized standards, European cybersecurity certification schemes, or common specifications by reference to which the conformity of the product is declared or by application of which its conformity is verified.

(6) From the placing on the market and for the support period contractually agreed for each product provided, or if no specification has been made for a support period of fifteen (15) years, the Supplier shall, in cases in which the Supplier knows or has reason to believe that the product provided or the processes put in place are not in conformity with the essential cybersecurity requirements, immediately take the corrective measures necessary to bring that product provided or the process concerned into conformity. If corrective measures are not commercially reasonable, the Supplier shall, as appropriate, withdraw or recall the product.

(7) If the product provided is radio equipment as defined in the Radio Equipment Directive (2014/53/EU) ("**RED**"), the product shall be constructed so as to ensure:

i. the protection of health and safety of persons and of domestic animals and the protection of property, including the objectives with respect to safety requirements set out in Directive 2014/35/EU, but with no voltage limit applying;

ii. an adequate level of electromagnetic compatibility as set out in Directive 2014/30/EU;

iii. that it both effectively uses and supports the efficient use of radio spectrum in order to avoid harmful interference.

(8) If the product provided is radio equipment as defined in the RED and falls within one of the following categories as specified by the Commission Delegated Regulation (EU) 2022/30 e, the Supplier shall ensure the following requirements:

i. Radio equipment that can communicate itself over the internet, whether it communicates directly or via any other equipment (internet-connected radio equipment): the radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service.

ii. Internet-connected radio equipment, if that equipment enables the holder or user to transfer money, monetary value or virtual currency: the radio equipment supports certain features ensuring protection from fraud.

b) Cybersecurity Risk Assessment

(1) The Supplier shall undertake an assessment of the cybersecurity risks associated with the product provided and take the outcome of that assessment into account during the planning, design, development, production, delivery and maintenance phases of the product with a view to minimizing cybersecurity risks, preventing incidents and minimizing the impacts of such incidents, including in relation to the health and safety of users. The cybersecurity assessment shall be conducted by an entity or individual who is officially trained and certified in cybersecurity risk assessment methodologies.

(2) The Supplier shall document and update the cybersecurity risk assessment as appropriate during the specified support period for the product provided.

(3) The cybersecurity risk assessment shall comprise at least an analysis of cybersecurity risks based on the intended purpose and reasonably foreseeable use, as well as the conditions of use, considering the length of time the product is expected to be in use.

(4) The cybersecurity risk assessment shall indicate the relevant regulatory security requirements and how those requirements are implemented.

c) Documentation

To the extent required by law, the Supplier shall establish the required technical documentation for the product provided and make it available to HARMAN immediately upon request.

d) Provision of Information

(1) The Supplier shall designate a single point of contact as specified in **Annex I** of the relevant Master Agreement or other relevant agreements (eg. SOW, Awards Letter, …) to enable HARMAN to communicate directly and rapidly with the Supplier, including in order to facilitate reporting on vulnerabilities of the product provided. The Supplier shall ensure that the single point of contact is easily identifiable.

(2) The Supplier shall ensure that the product provided is accompanied by the information and instructions to the user as set out in the applicable regulatory framework. The Supplier shall keep the information and instructions at the disposal of HARMAN and market surveillance authorities for at least fifteen (15) years after the product has been placed on the market or for the support period contractually agreed, whichever is longer. Where such information and instructions are provided online, the Supplier shall ensure that they are accessible, user-friendly and available online for at least fifteen (15) years after the product has been placed on the market or for the support period, whichever is longer.

(3) The Supplier shall provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for HARMAN.

(4) The Supplier shall ensure that the end date of the support period for the product provided, including at least the month and the year, is clearly and understandably specified at the time of purchase in an easily accessible manner and, where applicable, on the product provided, its packaging or by digital means. Where technically feasible in light of the nature of the product provided, the Supplier shall display a notification to HARMAN informing that the product provided has reached the end of its support period.

(5) If the Supplier ceases or is considering ceasing its operations and, as a result, would not able to comply with the applicable obligations concerning cybersecurity, it shall inform HARMAN of the impending cessation of operations of the relevant product provided by any

means available and to the extent possible, with reasonable notice before the cessation of operations takes effect.

e) Vulnerability Management, Incident Response, SLA

(1) The Supplier shall ensure, at the time of placing the product on the market and for the support period contractually agreed for each specific product provided, that vulnerabilities of that product, including its components, are handled effectively and in accordance with the essential cybersecurity requirements. The Supplier shall hereby ensure the following measures of vulnerability handling:

i. Identification and documentation of vulnerabilities and components contained in the product provided, including a software bill of materials ("**SBOM**") covering at the very least the top-level dependencies of the product. The SBOM shall be provided in a format acceptable to HARMAN, specifically SPDX 3.0 or higher or CycloneDX 1.4 or higher, and shall align with the minimum elements defined in the US NTIA SBOM guidelines. Where a Hardware Bill of Materials ("**HBOM**") has been provided or is contractually required, the SBOM shall be aligned with the HBOM to ensure consistency and comprehensive vulnerability management across both software and hardware components.

ii. Addressing and remediation of vulnerabilities without delay, including by providing security updates to eliminate the vulnerability.

iii. Effective and regular tests and reviews of the security of the product provided. The Supplier shall agree to black-box penetration testing conducted by HARMAN and, upon request from Harman, provide any evidence demonstrating the resilience of the product.

iv. Provision of information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities.

v. A policy on coordinated vulnerability disclosure.

vi. Measures to facilitate the sharing of information about potential vulnerabilities in the product provided, including by providing a contact address for the reporting of the vulnerabilities discovered in the product.

vii. Upon request and on a needed basis, HARMAN's development department may require the Supplier to take appropriate action regarding modifications or engineering changes necessary to address identified vulnerabilities.

(2) The Supplier shall have appropriate policies and procedures, including coordinated vulnerability disclosure policies, as required by law applicable to the provided product, to

process and remediate potential vulnerabilities that are either known to the Supplier or are intentionally or negligently unknown.

(3) The Supplier shall ensure that each security update concerning the product provided, which has been made available during the support period, remains available after it has been issued for a minimum of fifteen (15) years after the product has been placed on the market or for the remainder of the support period, whichever is longer. The Supplier shall implement secure mechanisms for distributing updates to the provided product to ensure that vulnerabilities concerning the product are promptly fixed or mitigated where necessary. Where applicable, security updates shall be deployed automatically. If security updates are available to address identified security issues, they shall be distributed without delay. Unless otherwise agreed between the Supplier and HARMAN for a tailor-made product with digital elements, security updates shall be provided free of charge. Each update shall be accompanied by an advisory message, providing HARMAN with relevant information, including potential actions to be taken.

f) Reporting Obligations

(1) The Supplier shall, upon identifying a vulnerability in a component, including in an open source-component, which is integrated in the product provided, immediately report the vulnerability affecting the product provided to HARMAN using the contact details specified by HARMAN in **Annex II** and address and remediate the vulnerability in accordance with the vulnerability handling requirements set out in this Framework. Where the Supplier has developed a software or hardware modification to address the vulnerability in that component, the Supplier shall share the relevant code or documentation with HARMAN, where appropriate in a machine-readable format.

(2) In the event of an incident, the Supplier will, if required by law, comply with the regulatory reporting obligations to the appropriate regulatory authorities and inform HARMAN accordingly.

V. ANNEX I: SUPPLIER INCIDENT NOTIFICATION CONTACT DETAILS

Contact Details of Responsible Persons
for Information Security and Business Continuity Management

The contact details of the Supplier are as follows:

Information Security

Corporate Name:	
Responsibility:	
Job Title:	
Group Mailbox:	
Telephone Number:	

Business Continuity Management

Corporate Name:	
Responsibility:	
Job Title:	
Group Mailbox:	
Telephone Number:	

Changes to the above details must be communicated to HARMAN via email at: tprm@harman.com

VI. ANNEX II: HARMAN INCIDENT NOTIFICATION CONTACT DETAILS

These email addresses must be used for notifying HARMAN of any potential or actual incidents as outlined in the agreement:

Product Security:	productsecurity@harman.com
IT Security:	itsecurity@harman.com

VII. Approval and Ownership

Review Approved By	Title	Date	Evidence
Natalie Kilber	Sr. Director, Product Security	04-June-2025	Approval Natalie.pdf

VIII. Revision History

Version	Date	Status	Author	Review Comments
1.0	12-Nov-2024	In use	Kornel Post	Initial Version, initial document named “HARMAN International Supplier Cybersecurity Framework”
1.1	04-Mar-2025	In use	Kornel Post	Adapted to new Structure based internal review
1.2	28-May-2025	In use	Marcel Sofian	Rename the document as “Product and Service Cybersecurity Policy” and added Approval evidence