Cybersecurity Management System (CSMS) Policy

DOCUMENT CONTROL

Document Title: Cybersecurity Management System (CSMS) Policy

Document ID: CSMS-POL-001

Document Type: Corporate Policy

Classification: Internal – Controlled

Owning Function: Enterprise Cybersecurity Office

Template Origin: Corporate Policy Template v3.4 (Legacy Word Format)

Primary Location: Internal Management System Repository

Supersedes: None (initial baseline document)

VERSION HISTORY

Version	Date	Author(s) / Contributor(s)	Description of Change	Audit Trigger
0.9	2019-11-14	Systems Assurance Group	Initial draft created to support emerging vehicle cybersecurity discussions	Internal gap review
1.0	2021-03-02	Enterprise Cybersecurity Office	Formalized as CSMS Policy; expanded lifecycle coverage	External readiness assessment
1.1	2022-09-18	Product Security & Compliance Team	Clarifications for post-production monitoring and role definitions	Customer audit
1.2	2024-06-27	Governance, Risk & Assurance Function	Alignment updates to ISO/SAE 21434 terminology; added limitations section	Certification audit

> *Note: Earlier versions of this document were maintained as unmanaged Word files prior to migration to the central repository.*

APPROVAL AND SIGN-OFF

Name / Role	Function	Signature	Date
Head of Enterprise Cybersecurity	Corporate Security	On file	2024-06-27
Director, Product Engineering	Engineering	On file	2024-06-28
Vice President, Quality & Safety	Quality & Functional Safety	On file	2024-06-28
Executive Sponsor	Senior Management	On file	2024-06-30

1. INTRODUCTION AND BACKGROUND

The increasing integration of electronic, software-based, and network-connected systems within road vehicles has resulted in an expanded exposure to cybersecurity risks across the organizational and product landscape. Over time, the organization has recognized that cybersecurity considerations can no longer be addressed solely at the technical implementation level, but instead require a structured, repeatable, and organization-wide management approach.

Historically, cybersecurity-related activities were executed in a decentralized manner, primarily driven by individual engineering teams or program-specific initiatives. While this approach provided localized risk mitigation, it did not consistently support enterprise-level visibility, accountability, or assurance. As regulatory expectations and customer requirements evolved, the need for a formal Cybersecurity Management System (CSMS) became evident.

This policy document represents a consolidation of practices, expectations, and governance mechanisms that have been incrementally developed over several years. It reflects both proactive planning and reactive adjustments made in response to audits, assessments, and observed gaps. As such, some sections may reiterate foundational concepts to ensure clarity and audit traceability.

2. PURPOSE AND OBJECTIVES

The purpose of this CSMS Policy is to define the organizational intent, principles, and high-level requirements for managing cybersecurity risks associated with products, services, and supporting processes throughout their lifecycle.

The objectives of this policy include, but are not limited to:

- Establishing a common understanding of cybersecurity responsibilities across the organization
- Providing a governance framework to support consistent cybersecurity risk management
- Demonstrating organizational commitment to cybersecurity to internal and external stakeholders
- Supporting compliance with applicable cybersecurity standards and regulatory expectations
- Enabling traceability between policy intent and supporting procedures, processes, and work products

This policy is written to support audit defense and evidence-based assessments. Accordingly, certain objectives are stated explicitly even where supporting mechanisms are defined in separate internal documents.

---

3. ORGANIZATIONAL SCOPE AND APPLICABILITY

This policy applies to all organizational units involved in the conception, development, production, operation, and support of vehicle-related systems and components that may influence cybersecurity risk.

Boilerplate Scope Statement (Legacy – Reused):

> *This policy applies to all personnel, departments, and activities involved in the design, development, production, operation, and maintenance of vehicle systems and associated services where cybersecurity considerations may reasonably apply.*

The scope includes, but is not limited to:

- Product engineering and systems development
- Embedded software and hardware design
- Manufacturing and production operations
- Aftermarket and post-production support functions
- Quality, safety, and compliance organizations
- Management and governance bodies

External parties such as suppliers and partners are considered indirectly within scope through contractual and interface requirements, as defined in referenced internal processes.

4. REGULATORY AND STANDARDS CONTEXT (HIGH-LEVEL)

The CSMS is informed by a range of international standards, industry guidelines, and regulatory frameworks related to cybersecurity and vehicle systems. While this policy does not reproduce detailed regulatory requirements, it establishes alignment at a conceptual level.

Relevant contexts include:

- Automotive cybersecurity standards addressing organizational and product-level risk management
- Broader information security management principles adapted for embedded systems
- Emerging regulatory expectations for lifecycle cybersecurity governance

Interpretation and detailed application of these external references are addressed in subordinate procedures and guidance documents maintained separately.

5. ORGANIZATIONAL CYBERSECURITY PRINCIPLES

The organization adopts the following cybersecurity principles as foundational to its CSMS:

1. **Risk-Based Approach**: Cybersecurity activities shall be proportionate to identified risks and potential impacts.
2. **Lifecycle Coverage**: Cybersecurity considerations shall be integrated across the entire product lifecycle.
3. **Defense in Depth**: Multiple layers of safeguards are preferred over reliance on single controls.
4. **Accountability**: Roles and responsibilities for cybersecurity shall be defined and communicated.
5. **Continuous Improvement**: The CSMS shall evolve based on monitoring, feedback, and lessons learned.

These principles are intentionally broad and may be interpreted differently across functions. Such variation is considered acceptable provided alignment with overall CSMS intent is maintained.

6. ROLES AND RESPONSIBILITIES

6.1 Cybersecurity Manager

The Cybersecurity Manager is responsible for overseeing the implementation and maintenance of the CSMS at an organizational level. This role includes coordination across departments, reporting to management, and serving as a focal point during audits.

Responsibilities may include:

- Maintaining CSMS-related policies and governance artifacts
- Supporting interpretation of cybersecurity requirements
- Coordinating internal assessments and reviews

6.2 Product Cybersecurity Lead

Each product or program is assigned a Product Cybersecurity Lead responsible for integrating cybersecurity considerations into product-specific activities.

Responsibilities include:

- Ensuring cybersecurity risk assessments are performed
- Acting as liaison between engineering teams and cybersecurity governance
- Supporting evidence generation for audits

6.3 Engineering Functions

Engineering functions are responsible for implementing cybersecurity requirements within their respective domains. This includes both system-level and component-level considerations.

6.4 Management Oversight

Management provides oversight by allocating resources, approving policies, and reviewing CSMS performance. Direct involvement may vary depending on organizational structure and maturity.

---

7. CYBERSECURITY ACROSS THE LIFECYCLE

7.1 Concept Phase

During the concept phase, high-level cybersecurity objectives and assumptions are identified. This may include preliminary threat considerations and architectural constraints.

7.2 Development Phase

Cybersecurity activities during development are more detailed and may include risk analysis, requirement definition, and verification planning. Documentation generated during this phase forms a significant portion of audit evidence.

7.3 Production Phase

In production, cybersecurity focus shifts toward configuration control, manufacturing integrity, and readiness for deployment. Interfaces with production quality processes are particularly relevant.

7.4 Post-Production Phase

Post-production activities include monitoring, incident response preparation, and update mechanisms. The extent of post-production cybersecurity activities may vary by product.

8. INTERFACES WITH QUALITY AND SAFETY PROCESSES

Cybersecurity activities interface with existing quality and functional safety processes. While these disciplines are distinct, coordination is necessary to manage overlapping risks and shared lifecycle milestones.

This interface is described at a high level in this policy and further detailed in referenced internal documents.

9. TRAINING AND AWARENESS

Cybersecurity awareness is promoted through a combination of formal training, role-specific guidance, and informal knowledge sharing. Training content and frequency may vary.

Records of training completion are maintained where required, though historical completeness may vary due to legacy practices.

---

10. MONITORING, REVIEW, AND CONTINUOUS IMPROVEMENT

The effectiveness of the CSMS is monitored through internal reviews, audit findings, and management feedback. Identified gaps may result in corrective actions or updates to policies and processes.

Continuous improvement is recognized as an ongoing objective rather than a fixed state.

---

11. DOCUMENT GOVERNANCE AND MAINTENANCE

This document is maintained under document control procedures. Updates are typically reactive, driven by audit outcomes or significant organizational changes.

Periodic review is intended but not always performed on a fixed schedule.

---

12. KNOWN LIMITATIONS AND ASSUMPTIONS

The CSMS is based on several assumptions, including stable organizational structures and consistent interpretation of roles. Limitations include reliance on referenced documents that may evolve independently.

ANNEX A – GLOSSARY

- **CSMS**: Cybersecurity Management System
- **Lifecycle**: Phases from concept through post-production
- **Risk**: Combination of likelihood and impact of a cybersecurity event

---

ANNEX B – ROLE DESCRIPTIONS

(Refer to Internal Document: ROLE-DEF-014 – Organizational Role Profiles)

ANNEX C – REFERENCED INTERNAL PROCESSES

- Cybersecurity Risk Assessment Procedure
- Product Development Lifecycle Process
- Incident Response Guideline
- Supplier Cybersecurity Interface Procedure