DENSO
Crafting the Core

POLICY NUMBER:
PO-IS-MA-01

COMPANY POLICY STATEMENT

SUBJECT:	***DMHU INFORMATION SECURITY POLICY***
VERSION NO.: 1	*EFFECTIVE DATE OF ISSUE: 5th July, 2023*

The information security policy of DENSO Manufacturing Hungary Kft.

Our organisation has assumed a leading role in the automotive industry in the field of the design and manufacturing of fuel supply systems, system control and engine control component parts and related services for decades. For this purpose, we strive for utmost diligence in managing the confidentiality, integrity and accessibility of information necessary for continuous and reliable operations and the scopes of responsibility and processes related thereto.

In order to meet the necessary and expected legal requirements and customer expectations, the company operates an information security management system in accordance with ISO/IEC 27001:2022 and the Trusted Information Security Assessment Exchange (TISAX) + VDA ISA 5.1 standards, that is monitored, reviewed and continuously improved under the direction of the chief information security officer (CISO).

I. Our Company is committed to maintaining an effective information security and data protection system that strictly complies with legal requirements, governmental decrees and social norms and that effectively protects the interests of our Company and our customers.

II. The Company shall establish and maintain an Information Security Control System with the full support of the senior management. The Company shall ensure, via its Information Security Policy, that its employees become cognizant of the importance of information security, so that they would be able to meet the Company's business requirements, protect its data and information and enforce information security considerations during the performance of their work. The information security system includes ensuring the continuity of production, the security of the data files managed and produced by the Company, the business intelligence of the Company, safeguarding the data of our partners and employees, and the management of the buildings, offices, equipment, transporting means and IT-systems.

III. We identify risks related to information security and make corresponding personal, systemic and technological counter-measures against the explored hazards. We evaluate the management of information security risks via annual review procedures, and ensure that the risks and their effects do not materially affect the operations of our Company, take appropriate measures to address identified risks and ensure that the hazards and their effects would not affect the operation of our Company substantially.

IV. We carry out continuous trainings and activities aimed at raising awareness in terms of information security based on the key principles and the conclusions deducted from any fortuitous incidents.

V. We will forthwith investigate all incidents related to information security and make coordinated efforts to minimise damage and prevent recurrences.

VI. Our company monitors the information security processes (product, resources, assets) and the continuous development and review of initiatives related to information security as well as maintaining their maturity levels and the further development thereof by regular assessment and analysis.

Székesfehérvár, 5th of July 2023

Masayuki Kitano
President

DENSO
Crafting the Core

POLICY NUMBER:
PO-IS-MA-01

VÁLLALATI POLITIKA

TÁRGY: ***DMHU INFORMÁCIÓBIZTONSÁGI POLITIKA***	
VERZIÓSZÁM.: 1.	*HATÁLYBALÉPÉS DÁTUMA: 2023. július 5.*

A DENSO Gyártó Magyarország Kft. információbiztonsági politikája

Szervezetünk. évtizedek óta meghatározó szerepet tölt be az autóiparban üzemanyag ellátó rendszerek, rendszer- és motorvezérlő alkatrészek tervezése, gyártása és a kapcsolódó szolgáltatások terén. Ennek érdekében kiemelt jelentőséggel kezeljük a folyamatos és megbízható működéshez szükséges információk bizalmasságának, sértetlenségének és hozzáférésének kezelését, illetve az ehhez kapcsolódó felelősségeket és folyamatokat.

A szükséges és elvárt törvényi követelmények és vevői elvárások teljesítésének az érdekében az ISO/IEC 27001:2022 szabvány, illetve a Trusted Information Security Assessment Exchange (TISAX) + VDA ISA 5.1 előírásaival összhangban a DENSO Gyártó Magyarország Kft. információbiztonság irányítási rendszert működtet, ennek működését nyomon követi, felülvizsgálja, és folyamatosan tovább fejleszti az információbiztonsági vezető (CISO) irányítása alatt.

VII. Vállalatunk határozott célja, hogy folyamatosan olyan hatékony információbiztonsági és adatvédelmi rendszert működtessen, amely szigorúan megfelel a törvényi, kormányzati jogszabályoknak és társadalmi normáknak és amely hatékonyan védi Vállalatunk és a Vállalat ügyfeleinek érdekeit.

VIII. A Vállalat a felsővezetés teljes támogatásával Információbiztonsági Irányítási Rendszert hoz létre és működtet. A Vállalat a kiadott Informatikai Biztonsági Szabályzat által biztosítja, hogy munkatársai megértsék az információbiztonság fontosságát, képesek legyenek a Vállalat üzleti elvárásait teljesíteni, adatainak és információnak védelmét megvalósítani és munkavégzésük során érvényesíteni tudják az információbiztonsági szempontokat. Az információbiztonsági rendszer kiterjed a termelés folytonosságának biztosítására, a Vállalat által kezelt és előállított adatállományok biztonságára, a Vállalat üzletviteli adatainak, partnereink és munkatársaink adatainak védelmére, a használt épületetek, irodák, berendezések, szállító eszközök és informatikai rendszerek kezelésére.

IX. Azonosítjuk az információbiztonsággal kapcsolatos kockázatokat és a feltárt veszélyforrásokra azoknak megfelelő személyes, szisztematikus és technológia ellenintézkedéseket hozzunk, Az információbiztonsági kockázatok kezelését éves felülvizsgálatokkal értékeljük, a feltárt veszélyforrásokra megfelelő intézkedéseket hozzunk és biztosítjuk, hogy a veszélyforrások, illetve azok hatásai Vállalatunk működését érdemben ne befolyásolják.

X. Folyamatos információbiztonsági tudatossági képzéseket és felvilágosító tevékenységeket folytatunk a főbb alapelvek és az esetleges incidensekből levont konklúziók alapján.

XI. Azonnal kivizsgálunk minden, az információbiztonsággal kapcsolatos incidenst és összehangolt erőfeszítéseket teszünk a károk minimalizálása és az újbóli előfordulások megelőzése érdekében.

XII. Vállalatunk rendszeres értékeléssel és elemzéssel ellenőrzi az információbiztonsági folyamatok (termék, erőforrás, eszközök) és az információbiztonsággal kapcsolatos kezdeményezések folyamatos fejlesztését és felülvizsgálatát, azok érettségi szintjeinek a megtartását és fejlesztését.

Székesfehérvár, 2023. július 5.

Masayuki Kitano
Elnök

DENSO
Crafting the Core

POLICY NUMBER:
PO-IS-MA-01

ПОЛІТИКА ПІДПРИЄМСТВА

СУБ'ЄКТ: **Політика інформаційної безпеки DMHU**	
ВЕРСІЯ NO.:. 1	*ДАТА НАБУТТЯ ЧИННОСТІ: 2023. július 5.*

Політика інформаційної безпеки ТОВ «Виробнича компанія DENSO Угорщина»

Наша організація протягом десятиліть відіграє визначну роль в автомобільній промисловості у сфері проектування та виробництва систем постачання палива, компонентів керування системою та двигуном, а також в області супутніх послуг. З цією метою ми надаємо великого значення управлінню конфіденційністю, цілісністю та доступністю інформації, необхідної для безперервної та надійної роботи, а також пов'язаній з цим відповідальності і процесам.

Щоб відповідати необхідним і очікуваним вимогам законодавства та очікуванням клієнтів, ТОВ «Виробнича компанія DENSO Угорщина» використовує систему управління інформаційною безпекою відповідно до стандарту ISO/IEC 27001:2022 і Trusted Information Security Assessment Exchange (TISAX) + VDA ISA 5.1. та контролює, переглядає й постійно вдосконалює її роботу під керівництвом керівника інформаційної безпеки (CISO).

I. Наша компанія ставить собі за мету підтримувати ефективну систему інформаційної безпеки та захисту інформації, яка суворо відповідає правовим, державним та суспільним стандартам і ефективно захищає інтереси нашої компанії та наших клієнтів.

II. Компанія створює та забезпечує функціонування Системи управління інформаційною безпекою за повної підтримки вищого керівництва. За допомогою виданої Політики безпеки інформаційної мережі Компанія гарантує, що її співробітники розуміють важливість інформаційної безпеки, здатні відповідати діловим очікуванням Компанії, здійснювати захист її даних та інформації, а також забезпечувати дотримання аспектів інформаційної безпеки під час своєї роботи. Система інформаційної безпеки включає в себе забезпечення безперервності виробництва, безпеку інформаційного фонду, якими керує та які створює Компанія, захист бізнес-даних Компанії, даних наших партнерів і співробітників, управління будівлями, офісами, обладнанням, транспортними засобами та IT-системами.

III. Ми визначаємо ризики, пов'язані з інформаційною безпекою, і впроваджуємо відповідні персональні, систематичні та технологічні заходи протидії виявленим джерелам небезпеки. Ми оцінюємо управління ризиками інформаційної безпеки за допомогою щорічних перевірок, вживаємо відповідних заходів щодо виявлених джерел небезпеки та гарантуємо, що джерела небезпеки та їхні наслідки істотно не впливають на роботу нашої Компанії.

IV. Ми проводимо постійні тренінги та навчальні заходи з питань усвідомлення інформаційної безпеки на основі ключових принципів та висновків, зроблених з можливих інцидентів.

V. Ми негайно розслідуємо всі інциденти, пов'язані з інформаційною безпекою, та докладаємо спільних зусиль для мінімізації збитків і запобігання їх повторенню.

VI. Наша компанія стежить за безперервним розвитком і переглядом процесів інформаційної безпеки (продуктів, ресурсів, інструментів) та ініціатив, пов'язаних з інформаційною безпекою, а також за підтримкою та розвитком рівня їх зрілості шляхом регулярної оцінки та аналізу.

м. Секешфегервар, 2023 липень 5.

Masayuki Kitano
Президент