DA-TOR
people forming progress

Headquarters
DA-TOR S.p.a.
via Provinciale 2
23879 Verderio (LC)
VAT N°: IT00571780139

Warehouse&Logistics
DA-TOR S.p.a.
via Marinetti
23879 Verderio (LC)
VAT N°: IT00571780139

German Branch
DA-TOR Automotive GmbH
Werner von Siemens-Straße 5
D-78166 Donaueschingen
VAT N°: DE322086794

Politica per la Sicurezza delle Informazioni

La Direzione di DA-TOR S.p.A. ("DA-TOR") con la predisposizione del presente documento, intende definire la Politica per la Sicurezza delle Informazioni precisandone gli obiettivi e gli impegni da essa derivanti.

SCOPO
La presente Politica si applica al perimetro TISAX di DA-TOR S.p.A. (Scope ID S24H50) e comprende tutti i processi, le procedure e le risorse sotto la responsabilità di DA-TOR rilevanti per la sicurezza degli oggetti di protezione (Protection Objects) e dei relativi obiettivi di protezione previsti dagli Assessment Objectives TISAX selezionati (High Availability e Confidential, Assessment Level 2).
Il perimetro comprende entrambi i siti oggetto di assessment: (i) DA-TOR S.p.A. - Produzione, Via Provinciale 2, 23879 Verderio (LC), e (ii) DA-TOR S.p.A. - Magazzino, Via Marinetti s.n.c., 23879 Verderio (LC). Nel perimetro sono inclusi il sistema informativo aziendale e tutte le attività di raccolta, memorizzazione ed elaborazione delle informazioni a supporto della produzione automotive di dadi, dadi per raccordo, dadi a saldare, dadi autobloccanti e boccole mediante stampatura, maschiatura e assemblaggio, nonché le correlate attività di magazzino e logistica.
Il campo di applicazione comprende inoltre i flussi informativi con la supply chain e con le altre parti esterne rilevanti ogniqualvolta queste scambino, accedano, elaborino, memorizzino, trasmettano o comunque trattino informazioni connesse ai processi inclusi nel perimetro. I requisiti di sicurezza applicabili governano pertanto anche i rapporti con fornitori, subfornitori, operatori logistici, fornitori ICT/di servizi, Clienti e altre terze parti, in funzione delle informazioni trattate, dei rischi associati e dei requisiti contrattuali.

Gli obiettivi di sicurezza delle informazioni perseguiti da DA-TOR, nell'ambito del perimetro di valutazione TISAX, sono:

- proteggere la riservatezza delle informazioni di Clienti, Fornitori e DA-TOR scambiate, raccolte, memorizzate ed elaborate nell'ambito dei processi di produzione e logistica, prevenendo accessi o divulgazioni non autorizzati;
- proteggere l'integrità e la tracciabilità delle informazioni utilizzate nei processi di stampatura, maschiatura, assemblaggio, supporto alla produzione e nelle attività di magazzino/logistica, prevenendo alterazioni non autorizzate o accidentali e garantendo che le informazioni rimangano accurate e affidabili lungo il loro ciclo di vita;
- assicurare la disponibilità delle informazioni, dei sistemi e dei servizi necessari a supportare le attività di Produzione e Magazzino/Logistica, riducendo probabilità e impatto degli incidenti di sicurezza e supportando la continuità dei processi interessati;
- proteggere le informazioni scambiate lungo la supply chain - inclusi Clienti, Fornitori, prestatori di servizi e altre parti esterne coinvolte nei processi in ambito - applicando requisiti di sicurezza proporzionati al rischio e ai requisiti contrattuali/del Cliente; • mantenere un Sistema di Gestione per la Sicurezza delle Informazioni coerente con ISO/IEC 27001:2022, TISAX/VDA ISA e con gli obblighi legali, regolamentari e contrattuali applicabili, perseguendo il miglioramento continuo e prestazioni di sicurezza misurabili.

Lo scopo è rappresentato dal perfezionamento delle procedure che possano garantire all'organizzazione di operare con maggiore efficienza, migliorare il controllo e la sicurezza delle attività e di raggiungere obiettivi sempre più sfidanti.
DA-TOR fornisce prodotti che si basano su risorse, incluse le informazioni. L'uso delle risorse informative deve essere in linea con le buone pratiche e procedure di lavoro, nonché con i requisiti legali, normativi e contrattuali e deve garantire la riservatezza, l'integrità e la disponibilità di tutte le risorse informative di DA-TOR e dei suoi Clienti.
L'informazione è un asset estremamente importante di DA-TOR e consente alla stessa di adempiere alle proprie funzioni e obblighi commerciali nei confronti delle controparti.
Il Sistema di Gestione per la Sicurezza delle Informazioni di DA-TOR garantisce che la stessa soddisfi i requisiti legali, regolamentari e contrattuali in materia di sicurezza delle informazioni, compresi quelli previsti dalla legge sulla protezione dei dati personali (Reg UE 2016/679, D.lgs. 101/18 e D.lgs. 196/03) e dal Garante Privacy.

In termini di Sicurezza dell'Informazione, nel dettaglio:
- l'approccio sarà basato sul rischio conformemente alla norma ISO/IEC 27001:2022 ed alle migliori pratiche;
- le procedure stabiliranno criteri di valutazione del rischio allineati con le attuali politiche di gestione del rischio strategico aziendale approvate da DA-TOR.

DA-TOR
people forming progress

Headquarters
DA-TOR S.p.a.
via Provinciale 2
23879 Verderio (LC)
VAT N°: IT00571780139

Warehouse&Logistics
DA-TOR S.p.a.
via Marinetti
23879 Verderio (LC)
VAT N°: IT00571780139

German Branch
DA-TOR Automotive GmbH
Werner von Siemens-Straße 5
D-78166 Donaueschingen
VAT N°: DE322086794

PRINCIPI DI SICUREZZA DELLE INFORMAZIONI

DA-TOR adotta i seguenti principi per la gestione della sicurezza delle informazioni:

- sicurezza by design e by default nei processi, nei sistemi e nei cambiamenti;
- accesso secondo i criteri need-to-know e least privilege;
- chiara attribuzione delle responsabilità e segregazione dei compiti ove appropriato;
- classificazione e protezione delle informazioni in funzione del loro valore, sensibilità e dei requisiti contrattuali; protezione basata sul rischio lungo l'intero ciclo di vita delle informazioni;
- scambio sicuro delle informazioni con Clienti e supply chain;
- protezione fisica e logica di siti, sistemi e asset; tempestiva rilevazione, segnalazione, gestione e analisi degli incidenti di sicurezza; resilienza, backup, ripristino e continuità proporzionati alle esigenze di business;
- controllo dei fornitori e delle terze parti lungo l'intero rapporto; consapevolezza e competenza del personale;
- rispetto dei requisiti legali, regolamentari e contrattuali; monitoraggio, audit, riesame della Direzione e miglioramento continuo del SGSI.

È precisa intenzione e compito della Direzione consolidare la consapevolezza interna verso gli obiettivi sempre più sfidanti della sicurezza delle informazioni, rafforzare l'immagine e la serietà aziendale, soprattutto attraverso la ricerca di trasparenza verso i propri Clienti, della professionalità che è riconosciuta alla società e di uno stile sempre più personalizzato ed esclusivo.
È quindi ferma volontà di DA-TOR implementare e seguire la presente Politica per la Sicurezza delle Informazioni affinché questa sia permeata ed attuata a tutti i livelli aziendali. La Società si impegna ad effettuare la formazione dei propri collaboratori in tal senso.
Questa Politica rappresenta l'impegno sul quale il Sistema per la Sicurezza delle Informazioni si basa.
Le linee guida e i requisiti della presente Politica si applicano a tutti i processi primari e di supporto ricompresi nel perimetro TISAX sopra definito, incluse le relative interfacce e gli scambi informativi con la supply chain e con le altre parti esterne.
È fatto obbligo a tutte le parti interessate di adottare adeguate misure di sicurezza in linea con i principi della presente politica.
Il mancato rispetto o la violazione dei principi di cui alla presente politica potrà dar luogo nei confronti del personale dipendente a provvedimenti disciplinari previsti dal CCNL, nonché all'applicazione di tutte le azioni civili e penali consentite, e per le parti interessate esterne alla revisione del rapporto contrattuale tra le parti fino alla risoluzione del contratto.
In particolare, la Direzione conferisce al Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni (RSGSI) la responsabilità di assicurare l'applicazione di quanto previsto e stabilito dal Sistema per la Sicurezza delle Informazioni e di tenere informata la Direzione stessa dei risultati scaturiti dai periodici Audit.
L'Alta Direzione riesaminerà periodicamente, in fase di Riesame della Direzione, le pratiche, le politiche e le linee guida correnti dell'azienda per raccomandare eventuali modifiche o miglioramenti al fine di garantire l'applicazione di misure di sicurezza appropriate.
La presente Politica è un documento controllato e viene mantenuto a disposizione del personale dipendente sul server in sola lettura e di tutte le parti interessate sul sito web. Il Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni (RSGSI) deve garantire che tutte le modifiche siano diffuse e che le copie obsolete siano rimosse e/o archiviate.
Assieme alla presente politica DA-TOR ha redatto specifiche politiche atte a regolamentare le seguenti tematiche: gestione degli incident, gestione della business continuity, gestione delle password, gestione del cambiamento, Regolamento sul corretto Utilizzo degli Strumenti Aziendali, gestione del backup e ripristino delle informazioni.

Verderio, 16/10/2026

DA-TOR
people forming progress
IL PRESIDENTE