

**Vimercati S.p.A.****Società a Socio Unico Soggetta a****Direzione e Coordinamento di****Viney Auto Ancillary Private Ltd. (art. 2497 bis c.c.)****Sede Legale**

20016 Pero (MI) - Italia

Via V. Monti, 38

<http://www.vimercati.com>e-mail: vimer@vimercati.compec: vimercatispa@pec.it

Capitale Sociale € 8.291.111

REA 1861504

Reg. Imp. Mi. C.F. e P. Iva 05938980967

V.A.T. Registration Number IT05938980967

Uffici e Stabilimento

20016 Pero (MI) – Italia

Via V. Monti, 38

Tel. +39 02 38194.1

Fax +39 02 38194331

Associata ANFIA

UNI EN ISO 9001:2015**IATF 16949:2016****ISO 14001:2015****ISO 45001:2023**

EMAIL & ACCESS MANAGEMENT POLICY

(Bilingual – IT / EN)

1. Finalità / Purpose

IT

La presente policy disciplina i criteri e le modalità di utilizzo delle caselle email aziendali, nonché la gestione dei relativi diritti di accesso. Gli obiettivi sono:

- garantire sicurezza informatica e continuità operativa;
- assicurare la protezione dei dati personali trattati tramite sistemi di posta;
- prevenire accessi non autorizzati e rischi di data breach;
- definire regole chiare di responsabilità;
- assicurare conformità alle normative vigenti.

EN

This policy defines rules for the use of corporate email accounts and the management of access rights.

Ensure cybersecurity and operational continuity;

Guarantee the protection of personal data processed through email systems;

Prevent unauthorized access and risks of data breaches;

Define clear rules of responsibility;

Ensure compliance with applicable regulations.

2. Titolarità delle caselle email / Ownership of Email Accounts

IT

Tutte le caselle email aziendali e i dati in esse contenuti sono di proprietà della Società e sono assegnati esclusivamente per finalità lavorative.

EN

All corporate email accounts and related data are company-owned assets and are provided exclusively for business purposes.

3. Diritti di accesso e deleghe / Access Rights and Delegations

IT

Tipologie di accesso: deleghe, shared mailbox, send as/on behalf, amministrazione IT. Tutti gli accessi devono essere autorizzati, registrati e limitati nel tempo. Vietato l'inoltro verso email personali.

Tali accessi devono essere formalmente autorizzati, limitati nel tempo e coerenti con il ruolo organizzativo.

Gli accessi temporanei concessi per transizioni organizzative devono essere revocati una volta cessata la necessità.

EN

Types of access: delegations, shared mailboxes, send as/on behalf, IT administration. All access must be authorized, logged, and time-limited. Forwarding to personal email accounts is prohibited.

Such access must be formally authorized, time-bound, and aligned with the organizational role.

Temporary access granted for organizational transitions must be revoked once no longer needed.

4. Principi di sicurezza / Security Principles

IT

La Società applica i seguenti principi: Minimo privilegio, minimizzazione dei dati, tracciabilità, segregazione ruoli, divieto controllo contenuti.

EN

The Company applies the following principles: minimum privilege, data minimization, traceability, role segregation, and prohibition of content monitoring.

5. Audit IT periodici / Periodic IT Audits

IT

La Società può effettuare audit tecnici periodici senza preavviso finalizzati a:

- verificare la correttezza delle configurazioni di accesso
- individuare accessi obsoleti o non più giustificati
- prevenire rischi di sicurezza e data breach

Gli audit:

- hanno natura esclusivamente tecnica e preventiva
- non prevedono la lettura dei contenuti delle email
- sono svolti preferibilmente in modo centralizzato sui sistemi IT

EN

The Company may carry out periodic technical audits without prior notice aimed at:

- verifying the correctness of access configurations
- identifying obsolete or no-longer-justified access rights
- preventing security risks and data breaches

The audits:

- are solely technical and preventive in nature
 - do not involve reading the content of emails
 - are preferably performed centrally on IT systems
-

6. Gestione delle anomalie / Handling of Anomalies

IT

Eventuali anomalie sono gestite prioritariamente con interventi tecnici correttivi.

Ogni ulteriore valutazione avviene solo se necessario e nel rispetto delle normative vigenti.

EN

Any anomalies are primarily handled through technical corrective actions.

Further evaluation is carried out only if necessary and in compliance with applicable regulations.

7. Assenze e cessazioni / Absences & Terminations

IT

Assenze: autoresponder ed eventuale delega.

Cessazioni: blocco immediato account e accesso tecnico limitato, ed eventuale delega.

EN

Absences: autoresponder and any delegation.

Terminations: immediate account blocking and limited technical access, ed eventually delegation.

8. Protezione dei dati e riservatezza / Data Protection and Confidentiality

IT

Le attività di audit sono svolte nel rispetto del GDPR e delle norme giuslavoristiche.

I risultati sono accessibili solo a personale autorizzato e conservati per il tempo strettamente necessario.

EN

Audit activities comply with GDPR and labor regulations.

Results are restricted to authorized personnel and retained only as long as necessary.

9. Ruoli e responsabilità / Roles and Responsibilities

IT

- IT Manager: attuazione della policy e conduzione degli audit
- Management: definizione del perimetro e supervisione
- Utenti: rispetto delle regole di accesso

EN

- IT Manager: policy implementation and audits
 - Management: scope definition and oversight
 - Users: compliance with access rules
-

10. Entrata in vigore / Entry into Force

IT

La policy entra in vigore alla data di approvazione da parte della Direzione.

EN

The policy enters into force on the date of approval by Management.

Pero, 18/02/2026

Firma D.G.
Riccardo Marra

