



Regolamento per la Sicurezza dell'Informazione



REGOLAMENTO PER LA SICUREZZA DELL'INFORMAZIONE

INDICE

0	REGISTRO DOCUMENTO	9
0.1	Registro indice di revisione documento.....	9
0.2	Registro modifiche documento.....	9
0.3	Redazione, riesame e approvazione.....	9
0.4	Lista di distribuzione.....	9
0.5	Termini e definizioni	9
1	SCOPO E CAMPO DI APPLICAZIONE	13
2	RIFERIMENTI NORMATIVI	15
3	GESTIONE DEGLI ASSET.....	17
3.1	Amministratore di sistema.....	19
3.2	Dispositivi	21
3.2.1	Computer desktop e computer portatili	21
3.2.2	Tablet e smartphone	23
3.2.3	Dispositivi mobili di connessione (internet key).....	27
3.2.4	Memorie di massa portatili	27
3.2.5	Stampanti, fotocopiatrici e fax	27
3.3	Rete dati.....	29
3.3.1	Internet.....	29
3.4	Software	31
3.4.1	Software proprietario.....	31
3.4.2	Software libero	33
3.5	Postazioni di lavoro	33
3.6	Controlli	35
4	ACCOUNT	38
4.1	Creazione e gestione degli account	39
4.1.1	Sistema ERP AS/400	41
4.2	Gestione e utilizzo delle password.....	41
4.2.1	Sistema ERP AS/400	43
4.3	Cessazione degli account	43
4.3.1	Sistema ERP AS/400	43
5	POSTA ELETTRONICA	44
5.1	Accesso alla posta elettronica del lavoratore assente.....	47
5.2	Eliminazione di un indirizzo di posta elettronica	49
6	SICUREZZA DEI FILE.....	51



Regolamento per la Sicurezza dell'Informazione

0	REGISTRO DOCUMENTO	9
0.1	Registro indice di revisione documento	9
0.2	Registro modifiche documento	9
0.3	Redazione, riesame e approvazione	9
0.4	Lista di distribuzione	9
0.5	Termini e definizioni	9
0	DOCUMENT LOG	10
0.1	Document revision index log	10
0.2	Document changes log	10
0.3	Writing, review and approval	10
0.4	Distribution list	10
0.5	Terms and definitions	10
1	SCOPO E CAMPO DI APPLICAZIONE	13
1	PURPOSE AND SCOPE	14
2	RIFERIMENTI NORMATIVI	15
2	NORMATIVE REFERENCES	16
3	GESTIONE DEGLI ASSET	17
3	ASSET MANAGEMENT	18
3.1	Amministratore di sistema	19
3.1	System administrator	20
3.2	Dispositivi	21
3.2.1	Computer desktop e computer portatili	21
3.2	Devices	22
3.2.1	Desktop computer and laptop computer	22
3.2.2	Tablet e smartphone	23
3.2.2	Tablet and smartphone	24
3.2.3	Dispositivi mobili di connessione (internet key)	27
3.2.4	Memorie di massa portatili	27
3.2.5	Stampanti, fotocopiatrici e fax	27
3.2.3	Connecting mobile devices (internet key)	28
3.2.4	Portable mass storage	28
3.2.5	Printer, copy machine and fax	28
3.3	Rete dati	29
3.3.1	Internet	29
3.3	Data net	30
3.3.1	Internet	30

6.1	Level of confidentiality of documents	52
6.2	Creation and management of encrypted or password protected files	52
6.3	Procedure Operative Standard (SOP).....	53
6.3	Standard Operative Procedures (SOP).....	54
6.4	Registro Trasferimento File	55
6.5	Accordo di Riservatezza (NDA).....	55
6.4	File Transfer Register.....	56
6.5	Non-Disclosure Agreement (NDA)	56
7	CONNESSIONI REMOTE FORNITORI.....	57
7	REMOTE CONNECTIONS WITH SUPPLIERS.....	58
8	SANZIONI.....	59
9	COMUNICAZIONI.....	59
8	SANCTIONS	60
9	COMMUNICATIONS	60
10	ELENCO DOCUMENTI	61
10	DOCUMENTS LIST	62

0 REGISTRO DOCUMENTO

0.1 Registro indice di revisione documento

rev.	Data	Descrizione della revisione
0.0	17/03/2021	Bozza per l'adeguamento del Regolamento Informatico (rev. 1.0.2) ai requisiti per la certificazione TISAX
1.0	21/05/2021	Prima emissione
1.1	30/06/2021	Aggiornamento elenco documenti
2.0	31/05/2024	Aggiornamento per allineamento contenuti a TISAX rev.5.1
2.1	25/06/2024	Specifiche per trasferimento file e NDA

0.2 Registro modifiche documento

Motivo	Promotore	Paragrafo	Modifica
Modulo M211 rinominato	EDP	9	Aggiornata Tabella 9-1
Aggiunta sottocapitoli 6.3, 6.4, 6.5	IT	6	

0.3 Redazione, riesame e approvazione

Redazione	Riesame	Approvazione
IT (<i>Mario Meroni</i>)	QHSE (<i>Roberto Ferrari</i>)	CIO (<i>Mauro Pizi</i>)

0.4 Lista di distribuzione

Tutti i process owner.

0.5 Termini e definizioni

I riferimenti alle informazioni documentate dei sistemi di gestione VIMERCATI sono evidenziati [in blu su sfondo grigio](#).

Valgono le sigle e gli acronimi riportati nella Tabella 0.5-1.

Sigla / Acronimo	Descrizione
CIO	Chief Information Officer
EDP	Electronic Data Processing
ERP	Enterprise Resource Planning
ICT	Information and Communications Technology
IT	Information Technology
QS	Sistema Qualità

Tabella 0.5-1 – Sigle e acronimi

1 SCOPO E CAMPO DI APPLICAZIONE

Il presente Regolamento definisce le norme di comportamento definite per:

- garantire la sicurezza dell'informazione, intesa come conservazione della riservatezza (disponibilità solo a persone o sistemi autorizzati), integrità (possibilità di modifica in modo consentito solo da parte di persone o sistemi autorizzati) e disponibilità (possibilità per le persone autorizzate di accedere quando necessario) delle informazioni che VIMERCATI gestisce e in essa circolano;
- tutelare i beni aziendali della VIMERCATI, dei suoi clienti e dei suoi fornitori;
- evitare condotte inconsapevoli o scorrette che potrebbero esporre VIMERCATI o terzi a violazioni di leggi o requisiti contrattuali, problemi di sicurezza, danni di immagine e danni patrimoniali,

che si applicano a tutti i processi aziendali connessi alla progettazione e produzione di complessivi elettromeccanici ed elettronici, interruttori, commutatori e moduli ergonomici (anche contenenti software) destinati all'industria automobilistica come prodotti di primo impianto o di ricambio.

L'osservanza del presente Regolamento è di primaria importanza per il corretto funzionamento della VIMERCATI, la sua reputazione di partner affidabile e la soddisfazione del cliente, elementi fondamentali per il successo e lo sviluppo dell'azienda.

A tale osservanza sono tenuti tutti i lavoratori VIMERCATI, ogni utente assegnatario di beni e risorse informatiche aziendali ovvero utilizzatore di servizi e risorse informative della VIMERCATI (es. dipendente, collaboratore, consulente, fornitore o altro) che operi in modo continuativo non occasionale all'interno della struttura aziendale utilizzandone beni e servizi informatici, tutti coloro i quali operano per conto o nel nome di VIMERCATI, tutti i fornitori di prodotti e servizi ai quali sia richiesto contrattualmente il rispetto del presente regolamento.

L'insieme delle norme di comportamento da rispettare è ispirato ai principi stabiliti nel Codice Etico VIMERCATI, compresi quelli di diligenza, informazione e correttezza nell'ambito dei rapporti di lavoro, ed è inoltre finalizzato a prevenire eventuali comportamenti illeciti dei dipendenti, pur nel rispetto dei diritti a essi attribuiti dall'ordinamento giuridico italiano.

A tale proposito si rileva che gli eventuali controlli previsti escludono finalità di monitoraggio diretto e intenzionale dell'attività lavorativa e sono disposti sulla base della vigente normativa, con particolare riferimento al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (Regolamento Generale sulla Protezione dei Dati, noto come GDPR), alla Legge 20 maggio 1970, n. 300 (Statuto dei lavoratori) e ai provvedimenti emanati dall'autorità garante per la protezione dei dati personali (in particolare al Provvedimento 1 marzo 2007, Trattamento di dati personali relativo all'utilizzo di strumenti elettronici da parte dei lavoratori).

2 RIFERIMENTI NORMATIVI

Il presente Regolamento è stato predisposto con specifico riferimento ai documenti riportati nella Tabella 2-1.

Documento	Titolo
Codice Etico VIMERCATI 29/09/2023	Codice Etico
Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016	Regolamento Generale sulla Protezione dei Dati (GDPR)
Legge 20 maggio 1970, n. 300	Statuto dei lavoratori
Decreto legislativo 8 giugno 2001, n. 231	Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300
Decreto legislativo 30 giugno 2003, n. 196	Codice in materia di protezione dei dati personali
Decreto legislativo 10 agosto 2018, n. 101	Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
Provvedimento dall'autorità garante per la protezione dei dati personali 1° marzo 2007	Trattamento di dati personali relativo all'utilizzo di strumenti elettronici da parte dei lavoratori
ISO/IEC 27001:2017	Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni – Requisiti
TISAX Participant Handbook Vers. 2.7.2	TISAX Participant Handbook
VDA ISA 5.1	Information Security Assessment

Tabella 2-1 – Riferimenti normativi

3 GESTIONE DEGLI ASSET

I beni e le risorse informatiche, i servizi ICT e le reti informative, costituiscono beni aziendali rientranti nel patrimonio sociale e sono da considerarsi di esclusiva proprietà VIMERCATI.

Il loro utilizzo è consentito solo per finalità di adempimento delle mansioni lavorative affidate a ciascun utente in base al rapporto in essere, ovvero per gli scopi professionali afferenti l'attività svolta per VIMERCATI e comunque per l'esclusivo perseguimento degli obiettivi aziendali.

A tal fine si precisa che ogni dato o informazione trattati per mezzo dei beni e delle risorse informatiche di proprietà VIMERCATI, sarà considerato come avente natura aziendale e conseguentemente non riservata.

Ogni utente è tenuto a salvaguardare i beni aziendali, custodendo in modo adeguato i beni mobili e immobili, le risorse tecnologiche e i supporti informatici, le attrezzature, i prodotti aziendali, le informazioni e/o il know-how VIMERCATI.

In particolare, ogni utente deve:

- usare i beni aziendali secondo le policy aziendali, osservando scrupolosamente tutti i programmi di sicurezza per prevenirne l'uso non autorizzato o il furto;
- evitare utilizzi impropri dei beni aziendali che possano essere causa di danno o di riduzione di efficienza, o comunque in contrasto con l'interesse della VIMERCATI;
- rispettare scrupolosamente quanto previsto dalla politica aziendale, al fine di non compromettere la funzionalità e la protezione dei sistemi informatici;
- non inviare messaggi di posta elettronica minatori e ingiuriosi, non ricorrere a linguaggio non educato o non professionale, non esprimere commenti inappropriati che possano recare offesa alla persona e/o danno all'immagine aziendale;
- custodire e non rivelare a terzi non autorizzati la propria password personale ed il proprio codice di accesso alle banche dati aziendali;
- non riprodurre per uso personale i software aziendali né utilizzare per fini privati gli strumenti in dotazione;
- segnalare tempestivamente all'amministratore di sistema o al proprio responsabile di riferimento, eventuali guasti, problemi tecnici o malfunzionamenti dei dispositivi.

VIMERCATI conferisce agli utenti la piena responsabilità del materiale aziendale concesso all'inizio e/o durante il rapporto lavorativo, ove per materiale si intendono tutti gli strumenti atti allo svolgimento della propria professione, quali personal computer, cancelleria, scrivania, smartphone, auto aziendali, dispositivi hardware di ogni genere e altro. Gli utenti di tale materiale sono tenuti conservare tali risorse economiche nel rispetto della VIMERCATI, il che include il mantenimento della propria postazione di lavoro in stato di cura e pulizia generale.

3.1 Amministratore di sistema

VIMERCATI conferisce all'amministratore di sistema il compito di sovrintendere ai beni e alle risorse informatiche e mobili aziendali. In particolare è compito dell'amministratore di sistema:

- gestire l'hardware e il software di tutti i dispositivi informatici e mobili di proprietà della VIMERCATI S.p.A.;
- provvedere alla sicurezza informatica dei sistemi informativi aziendali;
- gestire il ciclo di vita (creazione, attivazione, manutenzione, disattivazione) degli account di rete, e dei relativi privilegi di accesso alle risorse, assegnati agli utenti;
- creare, modificare, rimuovere o utilizzare qualunque account o privilegio (solo a fini di manutenzione o gestione della sicurezza e della protezione dei dati);
- monitorare il corretto utilizzo delle risorse di rete e dei dispositivi (applicativi inclusi) assegnati agli utenti (solo a fini di manutenzione o gestione della sicurezza e della protezione dei dati);
- rimuovere software e/o componenti hardware dalle risorse informatiche assegnate agli utenti (solo a fini di manutenzione o gestione della sicurezza e della protezione dei dati);
- utilizzare le credenziali di accesso di amministratore del sistema per accedere, anche da remoto, ai dati o alle applicazioni presenti su un dispositivo informatico assegnato a un utente, in caso di prolungata assenza, non rintracciabilità o impedimento dello stesso (solo se l'attività è disposta da un soggetto di VIMERCATI autorizzato o designato al trattamento dei dati personali all'interno di VIMERCATI e limitatamente al tempo strettamente necessario al compimento delle attività indifferibili per cui è stato richiesto).

L'elenco completo degli amministratori di sistema, contenente tutti i dati rilevanti, è disponibile presso la direzione, ed è aggiornato immediatamente in caso di modifiche ed è comunque rivisto annualmente (ogni 12 mesi).

All'amministratore di sistema fanno capo i compiti di monitoraggio della corretta fruibilità degli asset da parte dei dipendenti, dei relativi ripristini, aggiornamenti e/o manutenzioni necessari per lo svolgimento dell'operatività secondo qualità e sicurezza aziendali.

L'amministratore di sistema registra i dati sugli aggiornamenti dei dispositivi aziendali (es. censimento asset, aggiornamenti software e licenze).

3.2 Dispositivi

Per gli elaboratori, i sistemi informatici, i sistemi gestionali e i software che ospitano archivi di dati personali (o hanno accesso ad essi tramite la rete informatica):

- l'accesso agli incaricati ed agli addetti alla manutenzione è possibile solo in seguito ad autorizzazione scritta (se ente esterno);
- tutte le operazioni di manutenzione che sono effettuate in loco avvengono con la supervisione dell'incaricato del trattamento dei dati personali in oggetto o di un suo delegato;
- è vietato l'utilizzo sui personal computer di accessi remoti di qualsiasi tipo mediante modem e linee telefoniche, quando connessi alla rete aziendale.

Il trasferimento fisico di un elaboratore presso un laboratorio di riparazione, un fornitore o un cliente, è autorizzato solo a condizione che il destinatario dichiari per iscritto di avere redatto un documento sulla sicurezza e di aver adottato opportuni provvedimenti per la protezione dei dati presenti sul dispositivo. Durante il trasporto il dispositivo non deve mai essere lasciato incustodito e, nel caso in cui il trasferimento sia eseguito da un corriere, che questi non possa in alcun modo accedere al dispositivo.

3.2.1 Computer desktop e computer portatili

Per lo svolgimento delle proprie mansioni gli utenti utilizzano computer desktop e computer portatili di proprietà VIMERCATI e sono tenuti al rispetto delle seguenti regole:

- non è consentito modificare la configurazione hardware e software del proprio dispositivo se non previa esplicita autorizzazione dell'amministratore di sistema;
- non è consentito rimuovere, danneggiare o asportare componenti hardware;
- non è consentito installare autonomamente programmi informatici, applicativi e ogni altro software non autorizzato espressamente dall'amministratore del sistema;
- non è consentito all'utente del dispositivo caricare o inserire al suo interno dati personali non attinenti all'attività lavorativa svolta;

- è obbligo dell'utente cancellare in modo sicuro tutti i dati personali presenti sul dispositivo prima di consegnarlo all'amministratore del sistema o all'ufficio competente per la restituzione o una eventuale riparazione;
- è obbligo dell'utente del dispositivo, in relazione alle sue competenze lavorative, procedere con gli aggiornamenti del dispositivo richiesti dai software antivirus installati, nonché sospendere ogni attività in caso di minacce virus o altri malfunzionamenti, segnalandoli immediatamente all'amministratore di sistema;
- è obbligo dell'utente del dispositivo spegnere il dispositivo stesso al termine del suo utilizzo;
- è obbligo dell'utente dei computer portatili custodirli con diligenza e in modo protetto durante gli spostamenti, rimuovendo da essi gli eventuali files elaborati e salvati in locale, prima della loro riconsegna.
- Agli utenti che, per ruolo o tipologia di attività, necessitano di un collegamento remoto ai sistemi aziendali, viene fornito un accesso tramite VPN con autenticazione a doppio fattore, le credenziali delle VPN sono personali e non possono essere condivise.

3.2.2 Tablet e smartphone

Per alcuni ruoli, VIMERCATI mette a disposizione dispositivi mobili quali smartphone e tablet che consentono di usufruire sia della navigazione in Internet tramite rete dati che del servizio di telefonia tramite rete mobile.

Le specifiche relative ai limiti entro cui l'utente potrà utilizzare tali strumenti sono riportate nella scheda tecnica consegnata unitamente al dispositivo. L'utente dovrà attenersi ai suddetti limiti e in caso contrario potrà essere richiesto il rimborso dei costi sostenuti per il loro superamento.

Come per qualsiasi altra dotazione aziendale, il dispositivo mobile rappresenta un bene aziendale concesso in uso per scopi esclusivamente lavorativi. È tuttavia permesso un utilizzo personale sporadico e moderato dei telefoni aziendali utilizzando la "diligenza del buon padre di famiglia" prevista dalla normativa e comunque tale da non ledere il rapporto fiduciario instaurato con il proprio datore di lavoro.

Al fine di controllo del corretto utilizzo dei servizi di telefonia aziendale, VIMERCATI può esercitare i diritti di cui all'articolo 124 (Fatturazione dettagliata) del D. Lgs. n. 196 del 30-06-03, richiedendo ai provider di telefonia i dettagli necessari agli accertamenti sull'utilizzo del dispositivo e sui costi del traffico voce e dati effettuato. Tale controllo è eseguito secondo i criteri e le modalità descritte al § 3.6 del presente regolamento.

Qualora dall'esame del traffico voce e dati di una singola utenza si rilevasse uno scostamento significativo rispetto alla media del consumo, sarà richiesto il tabulato analitico delle chiamate effettuate dalla SIM in incarico all'utente per il periodo interessato.



Regolamento per la Sicurezza dell'Informazione

L'utente assegnatario di tablet e smartphone:

- è responsabile dell'uso appropriato dello stesso e della sua diligente conservazione;
- deve dotare il dispositivo di password di sicurezza con livello di protezione adeguato (es. codice PIN composto da almeno 4 cifre) che ne impedisca l'utilizzo da parte di altri soggetti;
- deve modificare la password di sicurezza con cadenza almeno semestrale e deve adottare tutte le opportune cautele per garantire la segretezza di tale password;
- che ritiene che un soggetto non autorizzato possa essere venuto a conoscenza della password di sicurezza del dispositivo a lui assegnato, deve immediatamente modificarla e comunicare a VIMERCATI la potenziale violazione della sicurezza del dispositivo. Nel caso tale violazione comporti possibili rischi per la privacy, VIMERCATI provvede ad attivare le procedure previste dal GDPR di notifica alle autorità, blocco dell'eventuale accesso fraudolento ed individuazione dei dati compromessi;
- che danneggia o smarrisce il dispositivo o ne subisce il danneggiamento o furto, deve immediatamente comunicare a VIMERCATI l'accaduto. Nel caso tale violazione comporti possibili rischi per la privacy, VIMERCATI provvede ad attivare le procedure previste dal GDPR di notifica alle autorità, blocco dell'eventuale accesso fraudolento ed individuazione dei dati compromessi, e si riserva la facoltà di attuare la procedura di cancellazione da remoto di tutti i dati sul dispositivo, rendendo il dispositivo stesso inutilizzabile e i dati in esso contenuti irrecuperabili: per tale scopo si utilizzano le procedure disponibili più idonee per lo specifico modello di dispositivo/sistema operativo (es. [blocco e reset dispositivo](#) per Android, [reset](#) per IOS (Apple)). Se l'accaduto è riconducibile a un comportamento negligente o imprudente dell'utente assegnatario o comunque a sua colpa nella custodia del bene, egli sarà ritenuto unico responsabile dei danni derivanti;
- non può caricare o inserire all'interno del dispositivo o della carta SIM del dispositivo qualsiasi dato personale non attinente all'attività lavorativa svolta, così come fare fotografie, riprese video, registrazioni audio non attinente all'attività lavorativa svolta e preventivamente autorizzate da VIMERCATI;
- deve cancellare tutti i dati presenti nel dispositivo o nella carta SIM del dispositivo, prima di consegnare lo stesso all'ufficio competente per la sua restituzione o un'eventuale riparazione;
- salvo diversi specifici accordi derivanti da esigenze di servizio, deve verificare che il sistema di geolocalizzazione del dispositivo sia disattivato (ove possibile), consapevole che in caso contrario VIMERCATI può venire a conoscenza, seppur incidentalmente, dei dati relativi alla posizione del dispositivo stesso e conseguentemente dell'utente assegnatario;
- non può installare applicazioni (gratuite o a pagamento) che non siano state preventivamente autorizzate da VIMERCATI.

3.2.3 Dispositivi mobili di connessione (internet key)

Agli utenti di dispositivi portatili (es. computer portatile, tablet) può essere concessa in dotazione anche una chiavetta per la connessione alla rete aziendale per consentire lo svolgimento delle mansioni lavorative da remoto.

I suddetti dispositivi mobili di connessione possono essere utilizzati esclusivamente sui dispositivi portatili forniti in dotazione da VIMERCATI, non è consentito utilizzarli su dispositivi personali o di terzi, e non è consentito concederne l'utilizzo a terzi.

Le specifiche relative ai limiti entro cui l'utente può utilizzare il servizio offerto tramite la chiavetta sono riportate nella scheda tecnica consegnata all'utente unitamente al dispositivo. L'utente dovrà attenersi ai suddetti limiti: in caso contrario potrà essere richiesto il rimborso dei costi sostenuti per il loro superamento.

3.2.4 Memorie di massa portatili

Per memorie di massa portatili si intendono tutti quei dispositivi che consentono di copiare e archiviare dati (es. cartelle, documenti, file in genere) da dispositivi informatici: CD-ROM, DVD, chiavi USB, schede di memoria, lettori mp3, fotocamere digitali, dischi rigidi esterni, ecc.

L'utilizzo di memorie di massa portatili personali non è consentito, se non preventivamente autorizzato per iscritto da VIMERCATI.

Le memorie di massa portatili utilizzate per trasferire o archiviare categorie particolari di dati personali (art. 9 del Reg. CE n. 679/2016 del 27-04-16) o relativi a condanne penali e reati (art. 10 del Reg. CE n. 679/2016 del 27-04-16), devono essere custodite dall'utente in modo sicuro e controllato (es. in armadi chiusi a chiave), per garantire che il loro contenuto non sia trafugato o modificato o distrutto.

Le memorie di massa portatili autorizzate, una volta connesse all'infrastruttura informatica VIMERCATI sono soggette (ove ciò sia compatibile) al presente Regolamento.

3.2.5 Stampanti, fotocopiatrici e fax

L'utilizzo di stampanti, fotocopiatrici e fax è consentito solo per scopi professionali. Non è consentito un utilizzo per fini diversi o privati, salvo una specifica autorizzazione da parte dell'ente.

Le stampe lanciate su stampanti, locali o condivise, non devono essere lasciate incustodite ma devono essere ritirate immediatamente dopo che sono state eseguite.

L'utilizzo del fax per l'invio di documenti confidenziali/riservate è consentito solo nel caso sia assolutamente necessario e non possa essere sostituito da un metodo meglio tracciato (es. e-mail). In tal caso, il destinatario dell'invio deve essere preventivamente avvisato e deve essere a lui richiesta conferma telefonica che i documenti siano stati ricevuti e che persone non autorizzate non siano venute a conoscenza del contenuto di detti documenti.

Stampanti, fotocopiatrici e fax dotati di memoria, connessi o meno in rete, sono gestiti dall'amministratore di sistema che provvede alla cancellazione periodica del loro contenuto e a tutte le operazioni ritenute necessarie per garantirne la sicurezza.

3.3 Rete dati

3.3.1 Internet

Gli utenti che, per lo svolgimento delle proprie attività, sono stati abilitati all'accesso ad Internet devono prestare particolare attenzione e adottare un utilizzo consapevole della rete così come dei servizi collegati, in quanto ogni operazione posta in essere è associata all'indirizzo IP assegnato a VIMERCATI.

La connessione a Internet, in quanto strumento a disposizione degli utenti per uso professionale, deve essere utilizzata in maniera appropriata, tenendo presente che ogni sito web può essere governato da leggi diverse da quelle vigenti in Italia; ciò deve essere tenuto in considerazione in modo da prendere ogni precauzione conseguente.

In particolare:

- l'utilizzo di Internet è consentito esclusivamente per scopi aziendali e pertanto non è consentito navigare su siti non attinenti allo svolgimento delle proprie mansioni lavorative;
- non è consentita l'effettuazione di qualsiasi genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisto on-line e simili, salvo casi espressamente autorizzati da VIMERCATI;
- è vietata ogni forma di registrazione su siti i cui contenuti non siano legati all'attività lavorativa;
- non sono permesse, se non per motivi professionali, la partecipazione a forum, l'utilizzo di chat, l'utilizzo di bacheche elettroniche e le registrazioni in guest-book, anche utilizzando pseudonimi (o nicknames);
- non è consentita la navigazione su siti e la memorizzazione di documenti informatici da siti, di natura oltraggiosa, pornografica, pedopornografica o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale o politica;

- è consentito l'utilizzo di soluzioni di Instant Messenger o chat esclusivamente per scopi professionali e attraverso strumenti e software messi a disposizione da VIMERCATI;
- non è consentito l'utilizzo di sistemi di social networking sul luogo di lavoro o durante l'orario lavorativo;
- non è consentito lo scambio o la condivisione di materiale audiovisivo, cinematografico, fotografico, informatico o altro anche se non protetto da copyright, utilizzando sistemi Peer-to-Peer, a qualsiasi titolo e anche se non a scopo di lucro.
- non è consentito sfruttare i marchi registrati, i segni distintivi e ogni altro bene immateriale di proprietà dell'ente in una qualsiasi pagina web o pubblicandoli su Internet, a meno che tale azione non sia stata preventivamente ed espressamente approvata.

È altresì proibito rigorosamente qualsiasi uso del Web che non trasmetta un'immagine positiva o che possa essere in qualunque modo essere nocivo all'immagine di VIMERCATI.

Per mezzo dell'amministratore di sistema e al fine di facilitare il rispetto delle predette regole, VIMERCATI si riserva la facoltà di configurare specifici filtri che inibiscono l'accesso ai contenuti non consentiti, con esclusione dei siti istituzionali, e che prevengono operazioni non correlate all'attività lavorativa (es. navigazione, download e upload di file o software).

3.4 Software

3.4.1 Software proprietario

L'installazione e l'utilizzo di software privi di regolare licenza non sono consentiti in nessun caso.

L'utilizzo di software proprietario è consentito nei limiti specificati nel rispettivo contratto di licenza d'uso. In particolare è vietata la duplicazione del software e della relativa documentazione.

Considerato quanto disposto dalle normative a tutela della proprietà intellettuale e del diritto d'autore, le persone coinvolte nella riproduzione illegale del software sono responsabili sia civilmente che penalmente e quindi soggette alle sanzioni previste dalla legge che comprendono il risarcimento del danno, il pagamento di multe e anche la reclusione.

La duplicazione illegale del software non è giustificabile e non è tollerata, costituisce violazione del presente regolamento ed espone alle sanzioni disciplinari previste.

La richiesta di dotarsi di software o applicativi che non sono presenti nella dotazione del dispositivo assegnato, deve essere formalmente presentata dall'utente al proprio responsabile di riferimento, il quale ne valuterà l'aderenza alla politica, la necessità rispetto al ruolo ricoperto in azienda e (ove applicabile) le caratteristiche tecniche.

3.4.2 Software libero

L'installazione e l'utilizzo di software libero (es. freeware, shareware) devono essere preventivamente autorizzati dall'amministratore di sistema.

3.5 Postazioni di lavoro

Per postazione di lavoro s'intende il complesso unitario di dispositivi (computer desktop, computer portatile, smartphone, accessori, periferiche e ogni altro dispositivo concesso in utilizzo all'utente). L'assegnatario di tali beni e strumenti informatici aziendali ha il compito di farne un uso responsabile, professionale e compatibile con i principi di diligenza sanciti nel codice civile.

Ogni dispositivo che compone la postazione di lavoro, sia esso acquistato, noleggiato o affidato in locazione, rimane di esclusiva proprietà di VIMERCATI ed è concesso all'utente per lo svolgimento delle proprie mansioni lavorative e comunque per finalità strettamente attinenti l'attività svolta.

Le postazioni di lavoro non devono essere mai lasciate incustodite con le sessioni utenti attive: a tal fine le policy di dominio impongono l'attivazione del salvaschermo e il blocco del pc dopo 15 minuti di inattività (per lo sblocco del pc è necessario l'inserimento della password di accesso) ed ogni utente che si allontana dalla propria postazione di lavoro deve bloccare la sessione in corso con il salvaschermo protetto da password o effettuare il logout dalla sessione.

VIMERCATI si riserva la facoltà di rimuovere d'ufficio e senza alcun preavviso qualsiasi dispositivo o software la cui installazione non sia stata prevista e/o autorizzata.

I dispositivi di proprietà personale dell'utente quali computer portatili, telefoni cellulari, smartphone, agende palmari, memorie di massa portatili, lettori musicali, fotocamere digitali, ecc. non possono essere collegati ai dispositivi delle postazioni di lavoro o alle reti informatiche aziendali, salvo preventiva autorizzazione scritta di VIMERCATI.

3.6 Controlli

VIMERCATI esclude la configurabilità di forme di controllo aziendali aventi direttamente come oggetto l'attività lavorativa dell'utente, in linea con quanto prescritto dall'ordinamento giuridico italiano (L. n. 300 del 20-05-1970, articolo 4) ma non esclude che si possano utilizzare sistemi informatici, impianti o apparecchiature dai quali derivi la possibilità di controllo a distanza dell'attività dei lavoratori per ragioni organizzative e produttive ovvero per esigenze dettate dalla sicurezza del lavoro. Per tali evenienze, eventualmente, sarà onere di VIMERCATI sottoporre tali forme di controllo all'accordo con le rappresentanze sindacali aziendali. In difetto di accordo e su istanza di VIMERCATI sarà l'ispettorato del lavoro a indicare le modalità per l'uso di tali impianti.

I controlli posti in essere saranno sempre tali da evitare ingiustificate interferenze con i diritti e le libertà fondamentali dei lavoratori e non saranno costanti, prolungati e indiscriminati.

VIMERCATI, riservandosi il diritto di procedere a tali controlli sull'effettivo adempimento della prestazione lavorativa nonché sull'utilizzo da parte degli utenti dei beni e dei servizi informatici aziendali (articoli 2086, 2087 e 2104 del codice civile italiano), agirà in base al principio della gradualità.

In attuazione di tale principio:

- i controlli saranno effettuati inizialmente solo su dati aggregati riferiti all'intera struttura aziendale ovvero a singole aree lavorative;
- nel caso in cui si dovessero riscontrare violazioni del presente regolamento, indizi di commissione di gravi abusi, illeciti o attività contrarie ai doveri di fedeltà e diligenza, verrà diffuso un avviso generalizzato o circoscritto all'area o struttura lavorativa interessata, relativo all'uso anomalo degli strumenti informatici aziendali, con conseguente invito ad attenersi scrupolosamente alle istruzioni ivi impartite;
- nel caso in cui siano rilevate ulteriori violazioni, si potrà procedere con verifiche più specifiche e puntuali, anche su base individuale.

VIMERCATI non può in alcun caso utilizzare sistemi da cui derivino forme di controllo a distanza dell'attività lavorativa che permettano di ricostruire l'attività del lavoratore.

3.7 Ticketing – Gestione assistenza

La gestione dei ticket di assistenza è fondamentale per fornire un supporto efficiente e organizzato agli utenti. Il sistema di ticketing consente di tracciare, gestire e risolvere richieste di supporto in modo sistematico.

Vimercati ha implementato un sistema di Ticketing personalizzato basato su OS-Ticket, e configurato secondo lo schema seguente.

Componenti del sistema di Ticketing

- **Interfaccia di Richiesta (Portal Utente):**
 - Un portale dove gli utenti possono inviare richieste di supporto.
 - Moduli di contatto o email dedicati.
- **Sistema di Creazione e Gestione Ticket:**
 - Genera un numero di ticket unico per ogni richiesta.
 - Permette di assegnare, dare priorità e classificare i ticket.
- **Dashboard di Amministrazione:**
 - Permette agli operatori di visualizzare, aggiornare e risolvere i ticket.
 - Include strumenti di comunicazione interna ed esterna.
- **Database di Conoscenza:**
 - Archivia risposte a problemi comuni.
 - Facilita l'auto-risoluzione da parte degli utenti.
- **Reportistica e Analisi:**
 - Fornisce metriche su tempi di risposta e risoluzione.
 - Identifica trend e aree di miglioramento.

Processo di Gestione dei Ticket

- **Ricezione del Ticket:**
 - L'utente invia una richiesta tramite il portale.
 - Il sistema genera automaticamente un ticket con un numero unico.
- **Assegnazione e Priorità:**
 - Il ticket viene assegnato a un operatore o a un team.
 - Viene stabilita la priorità in base alla gravità e all'urgenza del problema.
- **Diagnosi e Risoluzione:**
 - L'operatore contatta l'utente se sono necessarie ulteriori informazioni.
 - Viene elaborata una soluzione e comunicata all'utente.
- **Chiusura del Ticket:**
 - Una volta risolto il problema, il ticket viene chiuso.
 - L'utente viene notificato e, in alcuni casi, può fornire feedback.
- **Follow-up e Feedback:**
 - Utilizzo del feedback per migliorare il servizio.

Ogni utente dispone di un proprio Accesso personalizzato al sistema di Ticketing.

Ogni mese vengono estratti report, analizzati i dati e generati KPI per studiare andamento degli eventi, migliorare le attività di assistenza e studiare metodi di prevenzione degli eventi.

4 ACCOUNT

4.1 Creazione e gestione degli account

Un account utente consente l'autenticazione dell'utilizzatore e di conseguenza ne disciplina l'accesso alle risorse informatiche aziendali per singola postazione lavorativa.

Gli account utenti vengono creati dall'amministratore di sistema e sono personali, cioè associati univocamente alla persona assegnataria. Ogni utente è responsabile dell'utilizzo del proprio account utente.

L'accesso al proprio account avviene tramite l'utilizzo delle credenziali di autenticazione (solitamente username e password), comunicate all'utente dall'amministratore di sistema, che le genera con modalità tali da garantirne la segretezza.

Le credenziali di autenticazione costituiscono dati aziendali da mantenere strettamente riservati e non è consentito comunicarne gli estremi a terzi, anche a soggetti in posizione apicale all'interno di VIMERCATI.

Una volta eseguito l'accesso, il ruolo disegnato specificatamente per l'utente garantisce l'utilizzo delle funzioni di sua pertinenza. Ogni transazione disponibile è altresì assoggettata ai privilegi di gestione o di sola lettura dei dati da essa trattati e la sua regolamentazione è descritta nei manuali rilasciati dai produttori.

Se l'utente ha il sospetto che le proprie credenziali di autenticazione siano entrate in possesso di altre persone o che venga fatto un utilizzo non autorizzato del proprio account e delle risorse a questo associate, deve immediatamente modificare la password e comunicare la potenziale violazione all'amministratore di sistema e al competente responsabile della privacy.

In caso di assenza improvvisa o prolungata di un utente e per:

- improrogabili necessità legate all'attività lavorativa,
- esigenze produttive,
- operatività delle risorse informatiche
- mantenimento e/o dimostrazione della conformità legislativa in materia ambientale e di salute e sicurezza dei lavoratori,

VIMERCATI si riserva la facoltà di accedere a qualsiasi dispositivo assegnato in uso all'utente, per mezzo dell'intervento dell'amministratore di sistema.

4.1.1 Sistema ERP AS/400

Per il corretto funzionamento delle applicazioni gestionali, gli utenti in AS/400 sono classificati in 3 tipologie di utenza:

- 1) utenza individuale: è la tipologia di utenza standard utilizzata ogni volta che sia possibile e consente un ristretto numero di transazioni;
- 2) utenza di gruppo: è la tipologia di utenza utilizzata per gruppi di persone aventi lo stesso tipo di ruolo e comporta un secondo livello di accreditamento che consente d'individuare lo specifico utente che sta accedendo al sistema ERP AS/400 con un'utenza di gruppo, attraverso il suo identificativo di dominio; ad ogni login e logout, AS/400 registra tutti gli elementi fondamentali di sistema operativo e gestionale legati alle utenze utilizzate.
- 3) utenza tecnica: è l'utenza utilizzata nelle estrazioni dati da AS/400 ad altri server; le credenziali sono ad esclusivo appannaggio di programmi e servizi che si attivano in background e non contengono transazioni eseguibili dalle altre tipologie di utenza.

4.2 Gestione e utilizzo delle password

Al primo accesso, l'utente deve modificare la password ricevuta dall'amministratore di sistema. Ove il sistema lo consenta, tale richiesta di modifica della password è impostata dall'amministratore di sistema in modo che sia generata in automatico dal sistema.

L'utente deve modificare la password ogni 6 mesi. Ove il sistema lo consenta, tale richiesta di modifica della password è impostata dall'amministratore di sistema in modo che sia generata in automatico dal sistema. L'intervallo è ridotto a 3 mesi nel caso di trattamento di dati personali (art. 9 del Reg. CE n. 679/2016 del 27-04-16) o relativi a condanne penali e reati (art. 10 del Reg. CE n. 679/2016 del 27-04-16).

La password definita dall'utente deve:

- contenere almeno 8 caratteri tra alfanumerici e caratteri speciali (es. £, \$, %, &); nel caso in cui il sistema imponesse un numero inferiore di caratteri, andrà utilizzato il numero massimo consentito);
- contenere almeno un carattere maiuscolo, un carattere minuscolo, un numero e un carattere speciale;
- non includere parti del nome, del cognome o ad essi facilmente riconducibili;
- non essere basata su nomi di persone, date di nascita, animali, oggetti o parole ricavabili dal dizionario (anche straniero) o che si riferiscano ad informazioni personali;

- essere diversa da almeno le ultime 4 precedentemente utilizzate;
- non contenere una sequenza di caratteri identici o gruppi di caratteri ripetuti;
- essere diversa da password utilizzate per servizi personali, al fine di evitare che la compromissione di un'utenza personale costituisca una vulnerabilità per la sicurezza aziendale.

La password deve essere protetta con la massima cura e riservatezza: scrivere la password su post-it o altri supporti non soddisfa tale requisito, compromette le misure di sicurezza previste, costituisce violazione del presente regolamento e comporta l'applicazione di sanzioni.

4.2.1 Sistema ERP AS/400

Le caratteristiche della password sono impostate dal sistema e non possono essere modificate per tipologia di utenza, applicazione o altro.

La password può avere una lunghezza da 2 a 8 digit e non prevede obbligo di numeri o caratteri speciali. Per le utenze individuali, la sua durata è di 120 giorni mentre per le utenze tecniche e di gruppo, non vi è scadenza.

Tali limitazioni offrono una maggiore garanzia di continuità di funzionamento alle utenze tecniche sempre attive in background.

4.3 Cessazione degli account

In caso di cessazione di un account (es. termine del rapporto di lavoro di utente con VIMERCATI), le credenziali di autenticazione sono disattivate dall'amministratore di sistema entro trenta (30) giorni dall'ultimo giorno di collaborazione dell'utente, ed entro novanta (90) giorni l'account dell'utente è eliminato.

4.3.1 Sistema ERP AS/400

In caso di cessazione di un membro di un utente di gruppo, i restanti membri devono modificare la password dell'utente di gruppo.

In caso di cessazione di tutti i membri di un utente di gruppo, l'utente di gruppo è disattivato.

5 POSTA ELETTRONICA

Ad ogni utente titolare di un account, VIMERCATI assegna una casella di posta elettronica individuale.

I servizi di posta elettronica devono essere utilizzati a scopo professionale: l'account e-mail è uno strumento di proprietà di VIMERCATI ed è conferito in uso per l'esclusivo svolgimento delle mansioni lavorative affidate.

Ad uno stesso utente possono essere assegnate più caselle di posta elettronica, che possono anche essere condivise con altri utenti dello stesso gruppo/ufficio/dipartimento. Tali caselle di posta elettronica devono essere utilizzate esclusivamente per la ricezione dei messaggi mentre per risposte e nuovi invii deve sempre essere utilizzata la casella personale.

VIMERCATI valuta caso per caso le eventuali richieste degli utenti di assegnazione di una casella di posta elettronica aggiuntiva per uso privato.

Attraverso le caselle di posta elettronica, gli utenti rappresentano VIMERCATI nei confronti di terzi e per questo motivo viene richiesto un utilizzo della posta elettronica lecito, professionale e comunque tale da riflettere positivamente l'immagine aziendale.

Gli utenti sono responsabili del corretto utilizzo delle caselle di posta elettronica aziendale conformemente al presente Regolamento.

In particolare gli utenti devono:

- conservare le credenziali di accesso alla casella di posta elettronica, nella massima riservatezza e con la massima diligenza;
- mantenere la casella di posta elettronica in ordine, cancellando documenti inutili e allegati ingombranti;
- richiedere la conferma di lettura dei messaggi inviati;
- prestare attenzione alla dimensione degli allegati quando la posta elettronica è utilizzata per trasmettere file all'interno dell'organizzazione, privilegiando ove possibile il formato PDF;
- non aprire gli allegati provenienti da mittenti sconosciuti in quanto possono essere utilizzati come veicolo per introdurre programmi dannosi (es. virus), nel qual caso devono prima accertarsi dell'identità e attendibilità del mittente, e controllare mediante gli appositi software messi a disposizione (es. antivirus) gli allegati prima di aprirli;



Regolamento per la Sicurezza dell'Informazione

- rispondere alle e-mail pervenute solo da emittenti conosciuti e cancellare preventivamente le altre;
- collegarsi a siti internet contenuti all'interno di messaggi solo per motivate ragioni e quando sia comprovata la sicurezza del contenuto degli stessi.

Agli utenti non è consentito diffondere il proprio indirizzo e-mail aziendale attraverso la rete internet né utilizzare la casella di posta elettronica aziendale per inviare, ricevere o scaricare allegati contenenti video, brani musicali, ecc., salvo che questo non sia funzionale all'attività svolta per VIMERCATI (es. invio di presentazioni o materiali video aziendali).

Salvo l'utilizzo di appositi strumenti di cifratura, i sistemi di posta elettronica non possono garantire la riservatezza delle informazioni trasmesse. Pertanto si richiede agli utenti di valutare con attenzione l'invio di informazioni ad uso interno o riservate.

Nel caso in cui fosse necessario inviare a destinatari esterni informazioni riservate, gli allegati devono essere preventivamente crittati o protetti mediante apposito software (es. archiviazione e compressione con password). La chiave di crittazione/protezione (es. password per apertura e decompressione) deve essere comunicata al destinatario attraverso un canale diverso dall'e-mail (es. messaggio o chiamata telefonica) e mai assieme ai dati crittati.

Informazioni, dati personali e/o sensibili di competenza possono essere inviati soltanto a destinatari (persone o enti) qualificati e competenti.

I messaggi di posta elettronica devono contenere un avvertimento nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi e sia precisato che le risposte potranno essere conosciute da altri nell'organizzazione di appartenenza del mittente.

Le regole elencate nel presente paragrafo si applicano, ove compatibili, anche ad eventuali servizi di posta elettronica certificata.

5.1 Accesso alla posta elettronica del lavoratore assente

I client di posta elettronica messi a disposizione degli utenti assegnatari di una casella di posta elettronica, includono funzionalità per l'invio in caso di assenze programmate, di messaggi di risposta automatici contenenti i riferimenti dei soggetti aziendali in sostituzione con cui mettersi in contatto o a cui inviare le comunicazioni.

In caso di assenze non programmate (es. malattia) superiori a sette (7) giorni e qualora l'utente non abbia la possibilità di attivare i messaggi di risposta automatici (neanche avvalendosi dei servizi di webmail o della connessione da remoto alla propria casella di posta elettronica), VIMERCATI può disporre lecitamente mediante personale appositamente incaricato (Amministratore di Sistema ovvero un suo incaricato), l'attivazione dei messaggi di risposta automatici, notificandolo all'assente.

Nel caso in cui VIMERCATI necessiti di conoscere il contenuto dei messaggi di posta elettronica dell'utente resosi assente per cause improvvise o per improrogabili necessità legate all'attività lavorativa, si procede come segue:

- 1) un utente "fiduciario", inteso come lavoratore precedentemente nominato e/o incaricato per iscritto dall'utente assente, verifica il contenuto dei messaggi;
- 2) l'attività svolta dall'utente "fiduciario" è registrata in un apposito verbale e l'utente assente è informato alla prima occasione utile.

5.2 Eliminazione di un indirizzo di posta elettronica

In caso di interruzione del rapporto di lavoro con l'utente, l'indirizzo di posta elettronica è disabilitato entro trenta (30) giorni dalla fine del rapporto ed entro novanta (90) giorni l'indirizzo di posta elettronica è definitivamente cancellato.

VIMERCATI si riserva in ogni caso il diritto di conservare i messaggi di posta elettronica ritenuti rilevanti per le proprie attività.

6 SICUREZZA DEI FILE

Per garantire la sicurezza dei file (confidenzialità, integrità e disponibilità), Vimercati definisce come unico repository dei dati significativi i dischi di rete messi a disposizione degli utenti con le restrizioni definite dalla tipologia e ruolo.

I file non possono in alcun modo essere salvati unicamente in locale sul proprio dispositivo (pc, tablet ecc.).

6.1 Livello di riservatezza dei documenti

I documenti hanno tre livelli di riservatezza:

- **PUBBLICO:** documento che può essere distribuito a tutte le risorse VIMERCATI e all'esterno (inclusa pubblicazione su siti internet);
- **AD USO INTERNO:** documento che può essere distribuito a tutte le risorse VIMERCATI;
- **RISERVATO:** documento che può essere distribuito solo alle risorse (interne VIMERCATI e terze quali clienti e fornitori) che hanno necessità di accedervi per lo svolgimento delle proprie attività o, se applicabile, espressamente indicate dall'autore del documento.

La tipologia di protezione (password o crittazione) che i file devono avere per la trasmissione verso terzi dipende dalla classificazione del documento:

- i documenti pubblici e i documenti ad uso interno che non contengono informazioni riservate o dati sensibili, possono essere trasmessi in chiaro (es. materiale pubblicitario o informativo);
- i documenti riservati possono essere trasmessi protetti da password (es. informazioni relative a procedure di lavorazione) o crittati, il protocollo utilizzato per i trasferimenti file è SFTP.

I documenti contenenti dati sensibili che rientrano nello scopo del GDPR devono sempre essere protetti.

6.2 Creazione e gestione di file crittografati o protetti da password.

L'eventuale password utilizzata per proteggere i file deve rispettare le stesse regole definite al § 4.2 per le credenziali di accesso:

- contenere almeno 8 caratteri tra alfanumerici e caratteri speciali (es. £, \$, %, &); nel caso in cui il sistema imponesse un numero inferiore di caratteri, andrà utilizzato il numero massimo consentito);
- contenere almeno un carattere maiuscolo, un carattere minuscolo, un numero e un carattere speciale;

- non includere parti del nome, del cognome o ad essi facilmente riconducibili;
- non essere basata su nomi di persone, date di nascita, animali, oggetti o parole ricavabili dal dizionario (anche straniero) o che si riferiscano ad informazioni personali;
- essere diversa da almeno le ultime 4 precedentemente utilizzate;
- non contenere una sequenza di caratteri identici o gruppi di caratteri ripetuti;
- essere diversa da password utilizzate per servizi personali, al fine di evitare che la compromissione di un'utenza personale costituisca una vulnerabilità per la sicurezza aziendale.

Ove i programmi di generazione dei file lo permettano, deve essere impostata una password di lettura ed una, diversa, di modifica.

La password deve essere protetta con la massima cura e riservatezza: scrivere la password su post-it o altri supporti non soddisfa tale requisito, compromette le misure di sicurezza previste, costituisce violazione del presente regolamento e comporta l'applicazione di sanzioni.

Nel caso in cui, per scelta o per necessità, si proceda alla crittazione dei file, deve essere utilizzato uno dei programmi indicati dall'amministratore di sistema, impostandolo ad un livello di crittografia AES a 256 bit o equivalente.

Alla password di accesso al file crittografato si applicano le regole sopra scritte e valide per le password di protezione.

La password deve essere protetta con la massima cura e riservatezza: scrivere la password su post-it o altri supporti non soddisfa tale requisito, compromette le misure di sicurezza previste, costituisce violazione del presente regolamento e comporta l'applicazione di sanzioni.

6.3 Procedure Operative Standard (SOP)

Implementare queste pratiche e utilizzare i giusti strumenti e protocolli aumenta significativamente la sicurezza del trasferimento di file e proteggere i dati sensibili da accessi non autorizzati e perdite.

- Politiche di Backup: Assicurarsi che i file trasferiti siano sempre sottoposti a backup.
- Monitoraggio e Log: Tenere traccia di tutte le operazioni di trasferimento file per individuare eventuali attività sospette.
- Aggiornamenti di Sicurezza: Mantenere sempre aggiornati i software di trasferimento file e i protocolli di sicurezza per proteggere contro le vulnerabilità note.

6.4 Registro Trasferimento File

Il registro di trasferimento file è essenziale per tracciare e monitorare i trasferimenti di file in un ambiente sicuro. Questo registro può essere utile per diversi scopi, inclusi audit di sicurezza, risoluzione dei problemi e conformità normativa.

Per il trasferimento sicuro dei file viene utilizzato il protocollo SFTP, i programmi autorizzati da Vimercati devono supportare questo protocollo e garantire un sistema integrato di Logging per la tracciabilità dei trasferimenti, esempio: Filezilla, Winscp o programmi equiparabili.

6.5 Accordo di Riservatezza (NDA)

Per ogni trasferimento di file riservati verso terzi è necessario redigere il documento di riservatezza dei file, noto anche come accordo di non divulgazione (NDA - Non-Disclosure Agreement), è un contratto legale tra due o più parti che delinea informazioni confidenziali che le parti desiderano condividere tra di loro a scopo di collaborazione ma desiderano limitare l'accesso a terze parti.

Ove non sia già integrato negli accordi contrattuali fare riferimento al modello standard utilizzato da Vimercati.

7 CONNESSIONI REMOTE FORNITORI

Per quelle apparecchiature o sistemi di controllo che hanno la possibilità di accesso remoto, nel caso di situazioni di emergenza o interventi di manutenzione / aggiornamento delle macchine di produzione si può permettere l'accesso da parte dei fornitori.

Ogni richiesta di intervento remoto deve essere prima segnalata dal responsabile dell'attrezzatura al CIO, indicando la motivazione, la modalità e la durata prevista e successivamente autorizzata dal CIO stesso.

Ove possibile le connessioni devono avvenire tramite VPN con doppio fattore, dedicate e attivate allo scopo.

Nei casi in cui non sia possibile utilizzare tale modalità (es. software gestiti da sistemi proprietari che si connettono con i server dei fornitori) per mantenere la segregazione delle macchine, vengono attivati, sempre previa richiesta e convalida dei responsabili, collegamenti di rete temporanei, implementando il cablaggio delle schede di rete degli apparecchi di controllo.

In entrambi i casi i collegamenti vengono interrotti alla conclusione delle operazioni.

Queste operazioni di accesso e manutenzione coinvolgono il personale IT e della Manutenzione elettrica che garantiscono l'attivazione, la sicurezza e la disattivazione dei collegamenti, fisici e logici, secondo le modalità e le tempistiche richieste dal responsabile interno.

8 SANZIONI

La violazione di quanto previsto dal presente regolamento, rilevante anche ai sensi degli articoli 2104 e 2105 del codice civile italiano, può comportare l'applicazione di sanzioni disciplinari in base a quanto previsto dall'articolo 7 della Legge 20 maggio 1970 n.300.

Nel caso in cui sia commesso un reato o la cui commissione sia ritenuta probabile o solo sospettata, VIMERCATI avrà cura d'informare senza ritardo e senza necessità di preventive contestazioni o addebiti formali, le autorità competenti dell'utilizzo illecito o non conforme dei beni e degli strumenti informatici aziendali.

In caso di violazione accertata delle regole e degli obblighi esposti in questo regolamento da parte degli utenti, VIMERCATI si riserva la facoltà di sospendere, bloccare o limitare gli accessi di un account, quando appare ragionevolmente necessario per proteggere l'integrità, la sicurezza o la funzionalità dei propri beni e strumenti informatici e inoltre per impedire il reiterno di tale violazione.

Il presente regolamento, nella parte in cui contiene le regole per l'utilizzo dei beni e degli strumenti informatici aziendali e relativamente al trattamento di dati personali svolti dall'ente finalizzato all'effettuazione di controlli leciti, vale quale informativa ai sensi dell'articolo 13 del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016.

9 COMUNICAZIONI

Contestualmente all'assegnazione di un account, il presente regolamento è messo a disposizione degli utenti per consultazione.

La versione più aggiornata del Regolamento è pubblicata sia in formato elettronico che in formato fisico cartaceo allo scopo di facilitarne la diffusione a tutti gli interessati.

Ogni aggiornamento del presente Regolamento sarà notificato sulle bacheche aziendali e mediante l'invio di specifico messaggio e-mail; tutti gli utenti sono tenuti a conformarsi alla versione più aggiornata del Regolamento.

Le richieste di autorizzazione o concessione previste dal presente Regolamento possono essere inoltrate a VIMERCATI per mezzo di qualsiasi strumento che ne garantisca la tracciabilità (es. e-mail), a cui è riconosciuto il valore di forma scritta in modo del tutto analogo rispetto a quella cartacea.

10 ELENCO DOCUMENTI

I documenti elencati nella Tabella 9-1 sono parte integrante del presente Regolamento.

Sigla	Informazione documentata
P201	Gestione delle utenze
P202	Backup dei sistemi
P203	Gestione degli asset
P204	Gestione delle modifiche del sistema ERP
P205	Accesso alle sale macchine
P206	Antispam e SandBox
P207	Alta Affidabilità IT ed EDP
P208	Accesso Aree Prototipazione
P209	Sicurezza prototipi
M201	Accettazione e sottoscrizione del Regolamento per la Sicurezza dell'Informazione
M202	Assegnazione credenziali accesso
M203	Scheda Dati Utente
M204	Nomina Amministratore di Sistema
M205	Nomina Chief Information Officer
M206	Rapporto Controllo e Verifica Accessi
M207	Report Verifica Utenze
M208	Registro Accesso Locali Server
M209	Scheda Applicativi Gestionali
M210	Diagrammi di rete
M211	Richiesta Modifica Sistema/SW/ERP
M212	Gestione Modifiche
M213	Registro Competenze Sicurezza Informazione
M214	Registro movimentazione prototipi

Tabella 9-1 – Procedure e moduli/modelli