# REGOLAMENTO

**PER LA GESTIONE E L'UTILIZZO DEGLI STRUMENTI INFORMATICI**

**Indice delle Revisioni**

| Rev. | Data | Descrizione | Preparato da | Verificato da | Approvato da |
|---|---|---|---|---|---|
| 00 | | | | | |
| 01 | 19.03.2025 | Regolamento | | | |
| | | | | | |

**SOMMARIO**

1. PREMESSA ..... 3
2. AMBITO DI APPLICAZIONE ..... 3
3. SANZIONI ..... 3
4. DISPOSIZIONI GENERALI ..... 4
5. DISPOSITIVI INFORMATICI ..... 6
   I. Computer e altri dispositivi informatici ..... 6
   II. Smartphone ..... 7
   III. Fotocopiatrici, stampanti e scanner ..... 8
   IV. Supporti Rimovibili ..... 8
6. RETE INFORMATICA ..... 9
   I. Assegnazione e gestione delle credenziali di autenticazione ..... 9
   II. Rete internet ..... 9
7. POSTA ELETTRONICA – NAVIGAZIONE INTERNET ..... 10
   I. Posta elettronica ..... 10
   II. Navigazione in Internet ..... 13
8. SOCIAL NETWORK ..... **Errore. Il segnalibro non è definito.**
9. CHAT AZIENDALI ..... 14
10. PROTEZIONE ANTIVIRUS ..... 14
11. ACCESSO AI DATI TRATTATI DAL LAVORATORE - SISTEMI DI CONTROLLO ..... 14
12. DIVIETO DI REGISTRAZIONE ..... 15
13. DATA BREACH ..... 15
14. UTILIZZABILITA' IN GIUDIZIO ..... 16
15. DIRITTO ALLA DISCONESSIONE E RISPETTO DELLA VITA PRIVATA ..... 16
16. COMPORTAMENTO NEL RISPETTO DELLA PRIVACY ..... 16
17. REFERENTI IN MATERIA DI STRUMENTI INFORMATICI ..... 16
18. MODIFICHE ED INTEGRAZIONI ..... 17

# REGOLAMENTO
# PER LA GESTIONE E L'UTILIZZO DEGLI STRUMENTI INFORMATICI

## 1. PREMESSA

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete internet tramite computer o altri dispositivi messi a disposizione dei Lavoratori per lo svolgimento della propria attività, espone **Consorzio 2 Alto Valdarno** (di seguito denominata anche "CONSORZIO") e i Lavoratori stessi a rischi di natura patrimoniale, oltre alle responsabilità, anche penali, conseguenti alla violazione di specifiche disposizioni di legge - *in primis* in materia di diritto d'autore e di tutela dei dati personali (Reg. UE n. 679/2016 e D.Lgs. n. 196/2003 s.m.i.), creando evidenti problemi alla sicurezza, al patrimonio ed alla reputazione dell'Ente.

Premesso, quindi, che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi ai principi generali di, onestà, trasparenza, lealtà, diligenza liceità, correttezza e reciproco rispetto, il **Consorzio 2 Alto Valdarno** ha deliberato di adottare il presente Regolamento per la Gestione e l'Utilizzo degli Strumenti Informatici, volto sia a impedire usi impropri dei dispositivi messi a disposizione del personale, sia ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento di dati.

Con il presente Regolamento il **Consorzio 2 Alto Valdarno** intende salvaguardare la sicurezza del proprio sistema informatico e tutelare la riservatezza, l'integrità e la disponibilità delle informazioni e dei dati, anche personali, prodotti, raccolti o comunque trattati.

## 2. AMBITO DI APPLICAZIONE

a) Il presente Regolamento si applica a tutti i Dipendenti (senza distinzione di ruolo e/o livello) che vengano a contatto e/o utilizzino gli strumenti informatici dell'Ente, anche in caso di svolgimento dell'attività lavorativa al di fuori della sede di lavoro (ad es. in modalità "smart-working" o in trasferta).

b) Il rispetto delle prescrizioni contenute nel presente Regolamento costituisce parte integrante delle obbligazioni contrattuali alle quali i Lavoratori devono attenersi, secondo la diligenza richiesta nello svolgimento dell'attività lavorativa.

c) Le regole contenute nel presente Regolamento, si aggiungono ed integrano le specifiche istruzioni fornite al personale, in attuazione della normativa vigente per il trattamento dei dati personali, e completano le informazioni già fornite ai suddetti interessati in ordine alle modalità con cui potranno effettuarsi i necessari controlli o ai provvedimenti disciplinari conseguenti alle violazioni.

## 3. SANZIONI

La violazione delle disposizioni di cui al presente Regolamento può costituire un illecito e comportare la comminazione di sanzioni disciplinari, così come previsto dal Regolamento Disciplinare e/o dal

vigente CCNL, oltre all'addebito dei costi arrecati dagli abusi, salva ogni altra azione nelle sedi competenti civili e penali.

## 4. DISPOSIZIONI GENERALI

Gli utenti sono tenuti a servirsi delle risorse informatiche prestando il proprio contributo affinché ne sia preservata l'integrità e garantito il buon funzionamento.

Sono pertanto vietate:

a. attività contrarie alla legge nazionale, comunitaria e internazionale o proibite dai regolamenti e dalle consuetudini d'uso delle reti e dei servizi acceduti;
b. attività commerciali, o comunque lucrative, non autorizzate, nonché la trasmissione di materiale commerciale e/o pubblicitario non richiesto (*spamming*) o l'uso delle proprie risorse da parte di terzi per tali attività;
c. attività comunque idonee a danneggiare, distruggere, compromettere la sicurezza delle risorse informatiche del Consorzio o dirette a violare la riservatezza e/o cagionare danno a terzi, ivi inclusa la creazione, trasmissione e conservazione di immagini, dati o altro materiale offensivo, diffamatorio, osceno, indecente o che attenti alla dignità umana, specialmente se riguardante il sesso, la razza, la religione, le opinioni politiche o la condizione personale o sociale;
d. attività comunque non conformi ai fini istituzionali del Consorzio.

<u>Inoltre:</u>

a) Il Consorzio, in virtù del ruolo, delle responsabilità e delle mansioni conferite, può assegnare al Lavoratore un computer aziendale fisso e/o portatile, un telefono fisso e/o uno smartphone, eventuali ulteriori dispositivi informatici (quali a titolo esemplificativo tablet) funzionali allo svolgimento dell'attività lavorativa.

b) Presso gli uffici del Consorzio, inoltre, sono presenti fotocopiatrici, stampanti (plotter) e scanner in condivisione, accessibili e utilizzabili dai Lavoratori.

c) Qualora la mansione e/o il ruolo ricoperto non prevedano l'assegnazione di un dispositivo informatico individuale, il Consorzio mette a disposizione specifiche postazioni di lavoro dotate di computer, tastiera, mouse e monitor, da utilizzare anche in condivisione.

d) I dispositivi informatici aziendali, siano essi in condivisione o assegnati individualmente, sono meri strumenti di lavoro: ne è pertanto vietato l'utilizzo a fini personali e tutte le informazioni ivi contenute sono da considerarsi un bene aziendale e quindi di proprietà esclusiva del CONSORZIO. Sono vietati, pertanto, l'utilizzo per motivi personali e l'inserimento di dati privati, che potrebbero venire a conoscenza del Consorzio.

e) Il responsabile dei dispositivi informatici all'atto della consegna provvede a sottoporre al lavoratore un modulo di assegnazione e a riportare l'assegnazione nel relativo registro interno, per tenere traccia dei dispositivi. All'atto della riconsegna il responsabile sottopone al lavoratore modulo di riconsegna dei dispositivi (si rimanda alla lettera j). Il Responsabile IT dovrà inoltre registrare la creazione di eventuali account di servizio su dispositivi personali in modo da applicare quanto previsto al punto della lettera k).

f) Il Lavoratore è responsabile dei dispositivi informatici assegnati o usati in condivisione e deve custodirli con diligenza, sia durante l'utilizzo nel luogo di lavoro che negli spostamenti, evitando ogni possibile forma di danneggiamento. Il lavoratore è tenuto a servirsi delle risorse informatiche assegnate prestando il proprio contributo affinché ne sia preservata l'integrità e garantito il buon funzionamento. Qualora si verifichino danneggiamenti o malfunzionamenti, il Lavoratore è tenuto a darne tempestiva comunicazione al Responsabile IT.

g) Al fine di **prevenire** i **furti**, il Lavoratore deve garantire che i dispositivi informatici assegnati:

- non siano lasciati in luoghi non adeguatamente protetti (ad es. nell'automobile)
- in caso di viaggio in aereo, siano sempre trasportati come bagaglio a mano
- quando lasciati in albergo, siano consegnati al deposito valori o, quantomeno, riposti in una valigia o in un armadio chiusi a chiave.

In caso di furto o smarrimento dei dispositivi informatici, il Lavoratore è tenuto ad avvisare immediatamente il Responsabile IT, per eventuali azioni di disabilitazione, e a presentare denuncia alle Forze dell'Ordine, e copia della denuncia deve essere prontamente inviata al Responsabile IT e data comunicazione al DPO (si rimanda al punto 13).

h) In caso di **assenza dal servizio superiore a 60 giorni** il Consorzio si riserva la facoltà di chiedere la restituzione del dispositivo individuale eventualmente assegnato.

i) In ogni caso di **risoluzione del rapporto di lavoro**, il Lavoratore deve procedere alla contestuale riconsegna di tutti i beni e strumenti assegnatigli in uso individuale, che devono presentarsi in buono stato d'uso.

j) Con particolare riferimento ai computer portatili e agli altri dispositivi informatici aziendali eventualmente ottenuti in uso, al **momento della riconsegna** devono essere mantenute intatte le installazioni (programmi e applicativi) preesistenti – salvo aggiornamenti - ed il Lavoratore deve avere disabilitato le password di accesso ed eliminato eventuali file presenti in locale (es. Desktop o disco c) dopo averli salvati nelle cartelle di rete.

Alla riconsegna, il personale del servizio IT provvederà immediatamente a formattare i dispositivi informatici restituiti, al fine di cancellare i dati contenuti al loro interno e poterli assegnare.

k) **L'utilizzo di dispositivi personali per uso aziendale è vietato, salvo preventiva autorizzazione**. In tale ipotesi sarà necessaria la creazione da parte del servizio IT di un account di servizio, protetto, separato da quello privato, per evitare qualsiasi confusione e promiscuità tra dati personali e dati aziendali. In caso di cessazione del rapporto di lavoro, il lavoratore si impegna, prima di lasciare il CONSORZIO, a consentire al servizio IT di cancellare l'account di servizio, e tutti i suoi contenuti, e inoltre si impegna a non farne e/o conservarne copia alcuna. In caso di perdita del PC personale il lavoratore si impegna a darne immediata comunicazione al Responsabile IT e a sporgere denuncia ai carabinieri e sia darne comunicazione al DPO (si rimanda al punto 13).

## 5. DISPOSITIVI INFORMATICI

### I. Computer e altri dispositivi informatici

a) **Modalità d'uso del computer consortile**

Il Consorzio **non effettua il backup** dei dati memorizzati in locale sui pc, tranne che per quanto riguarda la posta elettronica installata su outlook.

I file creati, elaborati o modificati sui device assegnati, a garanzia della integrità dei dati ad es. in caso di rottura del device o perdita, devono essere salvati nei server consortili messi a disposizione dal Consorzio. Tutti i documenti per cui si renda necessaria la garanzia della conservazione devono essere posizionati sui server o copiati sugli stessi.

Le cartelle utenti presenti nei server del Consorzio sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi.

Qualunque file che **non** sia pertinente e legato all'attività lavorativa ***non può essere*** dislocato in queste unità.

Risulta opportuno che, con regolare periodicità (almeno ogni mese), ciascun utente provveda alla pulizia dei dispositivi informatici, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante in ossequio al principio della minimizzazione del trattamento dei dati.

b) I computer aziendali e gli altri dispositivi informatici assegnati individualmente o in condivisione presentano una serie di programmi e applicativi preinstallati che, salvo aggiornamenti automatici, non possono subire modifiche, implementazioni o disinstallazioni, se non su specifiche istruzioni del servizio IT.

Non è in alcun modo consentito l'uso o l'installazione di programmi, sistemi, applicativi e qualsivoglia strumento hardware, software o web-application diversi da quelli ufficialmente installati e/o non inerenti all'attività lavorativa. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'Ente a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (D. Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore. Nel caso fossero necessari ulteriori programmi, gli stessi dovranno essere autorizzati dal Responsabile IT.

Non è altresì consentito di modificare le caratteristiche e le configurazioni preimpostate, salvo specifiche autorizzazioni del servizio IT, cui compete di procedere in merito.

c) L'accesso ad ogni personal computer è protetto da password. Le password devono essere reimpostate immediatamente dall'utente all'assegnazione del dispositivo e devono essere

custodite dall'utente con la massima diligenza e non divulgate. È severamente vietato disabilitare la password di accesso.

d) **In caso di allontanamento temporaneo dal computer o dal dispositivo informatico, anche per breve e temporaneo inutilizzo, la postazione deve essere bloccata tramite la combinazione dei tasti WINDOWS + L, o in alternativa deve essere fatta la disconnessione del proprio utente in maniera tale da impedirne l'utilizzo a personale non autorizzato**.

e) Il **Personal Computer deve essere spento** prima di lasciare gli uffici o nel caso di assenza prolungata. Al termine del servizio i dispositivi aziendali e in particolare i computer devono essere spenti. Qualora si rendesse necessario eseguire delle elaborazioni durante la notte, il personale del servizio IT provvederà ad informare i Lavoratori coinvolti che non dovranno spegnere il dispositivo, ma bloccare la stazione di lavoro o attivare lo screen saver con password.

f) Il Consorzio rende noto che il personale del servizio IT è autorizzato a compiere interventi nel sistema informatico dell'Ente diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (a titolo esemplificativo ma non esaustivo, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware ecc.).

Detti interventi possono anche comportare l'accesso, in qualunque momento, ai dati trattati dai Lavoratori, ivi compresi gli archivi di posta elettronica, nonché la verifica sui siti internet visitati.

La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività del Consorzio, si applica anche in caso di assenza prolungata o impedimento del Lavoratore (v. *infra*)

g) Il personale incaricato del servizio IT ha la facoltà di collegarsi e visualizzare in remoto il desktop dei computer aziendali al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, ecc.

L'intervento di collegamento e visualizzazione da remoto viene effettuato su chiamata del Lavoratore o, in caso di oggettiva necessità, per intervento diretto del personale incaricato del servizio IT, a seguito della rilevazione tecnica di problemi nel sistema informatico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, ne verrà data informativa al Lavoratore interessato.

h) **Eventuale presenza di virus informatici**

I virus possono essere trasmessi tramite scambio di file via internet, via mail, scambio di supporti removibili, filesharing, chat ecc.

È necessario scollegare il device dalla rete contattare, immediatamente e senza ritardo, il referente Informatico del Settore Servizi Tecnici qualora si sospetti che il device assegnato risulti infettato da un virus informatico (ad esempio perché presenta un comportamento anomalo).

## II. Smartphone

a) In caso di assegnazione di smartphone e SIM dati, anche questi sono consegnati con una serie di programmi e applicativi preinstallati. Non è ammesso scaricare alcuna ulteriore app senza previa autorizzazione da parte del Responsabile IT.

b) Impostare un PIN numerico o l'impronta digitale per accedere al dispositivo medesimo, in modo da evitare accessi accidentali da parte di terzi.

c) Lo smartphone e la SIM aziendali devono essere restituiti in caso di cessazione del rapporto di lavoro. Il Lavoratore, anche in caso di utilizzo promiscuo, non ha alcun diritto alla portabilità dell'utenza telefonica intestata al CONSORZIO, che potrà eventualmente concederla su motivata richiesta a propria mera discrezione.

d) In quanto titolare dell'utenza, il Consorzio ha accesso ai tabulati contenenti i dati del traffico, ed avendo interesse al corretto utilizzo della SIM ed al monitoraggio dei costi, può effettuare periodicamente, nel rispetto delle garanzie e delle disposizioni previste in materia di Privacy, controlli quantitativi, al fine di verificare l'uso conforme alle direttive ed alle relative necessità operative e funzionali.

In caso di accertamento di anomalie e/o abusi nell'utilizzo, la concessione del telefono e della SIM card potrà essere revocata, e potrà altresì essere promosso procedimento disciplinare per uso indebito di strumenti aziendali, con addebito a carico del Lavoratore del traffico anomalo e privo di giustificazione.

## III. Fotocopiatrici, stampanti e scanner

a) Non lasciare nel vassoio della stampante i documenti stampati, ma a ritirarli prontamente al fine di evitare la possibile perdita o divulgazione delle informazioni negli stessi contenuti a persone non autorizzate.

b) Privilegiare la stampa dei documenti in modalità fronte/retro e bianco/nero.

c) Cancellare i file scansiti qualora siano stati depositati temporaneamente in cartelle comuni denominate, a mero titolo esemplificativo "scan" o "condiviso".

d) Non possono essere stampati, fotocopiati o scansiti con strumenti aziendali documenti aventi contenuto oltraggioso e/o discriminatorio per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica ovvero coperti e protetti dalla normativa sul diritto d'autore.

## IV. Supporti Rimovibili

a) È vietato l'utilizzo di supporti rimovibili personali all'interno del Consorzio e sui dispositivi aziendali. Sono ammessi i soli supporti autorizzati dal Responsabile IT, che dovrà tenerne traccia con indicazione degli assegnatari. I lavoratori ai cui sono stati assegnati tali supporti si impegnano a proteggere con password, create nel rispetto delle istruzioni ricevute, i file contenenti dati personali.

b) Gli eventuali supporti rimovibili aziendali (cd, dvd, supporti USB, hard disk esterni, ecc.), devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato, alterato, distrutto o, successivamente alla cancellazione, recuperato.

c) In assenza di specifiche autorizzazioni da parte della Direzione, i supporti rimovibili aziendali non devono essere duplicati e/o consegnati a terzi.

d) Eventuali perdite devono essere immediatamente segnalate al Responsabile IT e si deve procedere alla denuncia ai carabinieri, dando comunicazione al DPO (si rimanda al punto XI).

## 6. RETE INFORMATICA

### I. Assegnazione e gestione delle credenziali di autenticazione

a) Le credenziali di autenticazione per l'accesso alla rete aziendale vengono assegnate al Lavoratore dal Responsabile IT, e successivamente devono essere variate al primo utilizzo, e modificate periodicamente con cadenza semestrale.

b) Le credenziali di autenticazione consistono in un codice per l'identificazione del Lavoratore (User ID), associato ad una parola chiave riservata (password) che deve essere custodita con la massima diligenza e non divulgata, e non deve contenere riferimenti agevolmente riconducibili all'utilizzatore.

c) Va adottata ogni opportuna cautela per assicurare la segretezza della password; pertanto, è fatto divieto di:
- rivelare la password a terzi;
- annotare la password su documenti cartacei e/o digitali che possano – anche solo inavvertitamente – essere intercettati da soggetti terzi;
- usare la stessa password utilizzata per accedere a strumenti e/o applicativi personali.

Evitare di comporre la propria password in luoghi pubblici ovvero in presenza di altri soggetti che possano – anche solo inavvertitamente – entrare in possesso delle suddette credenziali di accesso, anche se dipendenti o collaboratori del Consorzio.

d) In caso di furto o smarrimento della password, di avvenuto accesso non autorizzato alla stessa ed in ogni altra situazione in cui la sicurezza della password sia stata compromessa, il Lavoratore deve comunicarlo immediatamente al Responsabile IT.

e) In caso di dimenticanza della password, è possibile chiedere al Responsabile IT il reset e l'assegnazione di nuove credenziali.

f) Il servizio IT può - qualora circostanze particolari lo richiedano ovvero per eventuali necessità di urgenza o di limitazione del rischio - variare le password di accesso a qualsiasi sistema aziendale in modo autonomo, informandone i Lavoratori interessati.

### II. Rete internet

a) Il Consorzio adotta idonee misure tecniche preventive volte a ridurre navigazioni a siti non correlati all'attività lavorativa attraverso filtri e black list (liste di siti vietati).

b) Per l'accesso alla rete del CONSORZIO ciascun Utente deve essere in possesso delle specifiche credenziali di autenticazione rilasciate dal Responsabile IT.

È proibito entrare nella rete e nei programmi aziendali con un codice d'identificazione Utente diverso dal proprio.

c) Le cartelle utenti presenti nei server del CONSORZIO sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi.

Pertanto, qualunque file o documento che non sia legato all'attività lavorativa non può essere salvato o conservato, nemmeno per brevi periodi, in queste unità.

Il servizio IT, durante le periodiche attività di controllo, amministrazione e back-up su tali cartelle, può procedere alla rimozione di ogni file o applicazione ritenuti pericolosi per la sicurezza sia dei computer che delle unità di rete, dandone comunicazione al Lavoratore che ne abbia effettuato la creazione e/o l'inserimento.

d) È vietato accedere ai siti internet mediante azioni inibenti dei filtri, sabotando o comunque superando o tentando di superare o disabilitando i sistemi adottati dal Consorzio per bloccare accessi non conformi. In ogni caso è vietato utilizzare software o altri strumenti che consentano la navigazione anonima o di bypassare tali filtri.

## 7. POSTA ELETTRONICA – NAVIGAZIONE INTERNET

### I. Posta elettronica

a) Anche le caselle di posta elettronica aziendale costituiscono uno strumento di lavoro, pertanto sono di esclusiva proprietà aziendale, ed i Lavoratori rispondono del loro corretto utilizzo.

b) Ai collaboratori esterni non è consentito l'utilizzo di mail con il dominio "*@altovaldarno.it*", riservato ai dipendenti ed agli organi sociali (Presidenza, OdV, ecc.).

c) Il CONSORZIO ha scelto di assegnare ai lavoratori caselle di posta elettronica nominative. Tuttavia, per garantire un'identificazione chiara e univoca, chi invia un'email è tenuto ad apporre in calce il proprio nome e cognome, specificando anche il settore, l'ufficio o l'area di appartenenza.

d) È fatto divieto di utilizzare le caselle di posta elettronica aziendali per motivi diversi da quelli strettamente legati all'attività lavorativa; parimenti è vietato utilizzare caselle di posta elettronica private e personali per ragioni lavorative. È, infatti, necessario, evitare qualsiasi promiscuità tra dati e informazioni di natura lavorativa e di natura privata.

e) In calce alle mail dell'Ente verrà inserito automaticamente un avviso (*disclaimer*) del seguente tenore, a tutela dei Lavoratori e dei terzi interlocutori, di cui è vietata la cancellazione: "*La presente casella di posta elettronica è uno strumento aziendale utilizzato per mere ragioni di servizio. Non sussiste pertanto alcuna "privatezza" della corrispondenza, che rimane nella libera disponibilità di accesso e lettura da parte dell'organizzazione aziendale, viene soggetta a backup e conservata in archivio quale patrimonio informativo del Consorzio per il tempo necessario alle finalità dei trattamenti previsti dalle normative in materia e delle pratiche in corso.*"

f) In caso di assenze programmate (ad esempio, per ferie, permessi, trasferte, ecc.), qualora vi sia un unico utilizzatore della casella di posta elettronica aziendale, questi è tenuto ad impostare un messaggio di risposta automatica "*out of office*" contenente i riferimenti di un contatto alternativo aziendale. Qualora il Lavoratore non sia nella possibilità di attivare personalmente tale funzionalità, può chiedere il supporto del Responsabile IT che procederà ad impostare il messaggio automatico di cui sopra, salvo poi, richiedere al Lavoratore interessato, la modifica della password di accesso al sistema.

g) In caso di assenza non programmata (ad es. per malattia), detta procedura - qualora non possa essere attivata dal Lavoratore - verrà attivata a cura del Consorzio tramite il Responsabile IT o il personale del servizio IT.

h) Qualora lo richiedano esigenze improrogabili di servizio, il Responsabile o comunque superiore gerarchico, tramite il servizio IT, potrà accedere al contenuto della mail aziendale utilizzata dal Lavoratore assente per verificarne il contenuto; ciò modificando la password di accesso e informandone per iscritto il Lavoratore, cui dovrà essere consegnata una nuova password, da modificare a sua cura al primo utilizzo successivo.

i) La casella di posta elettronica aziendale deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti. Tali documenti e allegati vanno salvati sulle apposite cartelle di rete.

j) La dimensione massima degli allegati delle e-mail in uscita è di 15/20 Mb. Qualora il Lavoratore avesse la necessità di inviare allegati di dimensioni superiori dovrà segnalarlo al Responsabile IT che verificherà la possibilità di inviare gli stessi attraverso altre modalità.

k) Gli eventuali controlli, compiuti dal personale incaricato del servizio IT nel rispetto della normativa vigente in materia di trattamento dei dati personali, saranno effettuati in conformità di quanto specificato nel presente Regolamento.

l) È vietato:

- l'invio automatico di e-mail all'indirizzo e-mail privato (attivando per esempio un "inoltro" automatico delle e-mail entranti), sia durante i periodi di assenza (es. ferie, malattia, infortunio ecc.) sia in caso di cessazione del rapporto di lavoro;
- copiare la corrispondenza aziendale su supporti esterni personali (divieto di back up su chiavetta o altro supporto).

Trattasi di misure finalizzate a garantire la riservatezza della corrispondenza aziendale ed evitare fuga di dati o notizie. Un eventuale inoltro effettuato in violazione del divieto, allorché scoperto durante le periodiche verifiche di sistema potrebbe essere sanzionato a dare adito a richieste risarcitorie da parte del Consorzio.

m) Va prestata la massima attenzione nell'inserimento dei destinatari in copia conoscenza negli invii delle mail: è onere di ciascuno verificare che non vengano condivise informazioni, dati personali ovvero altri contenuti con destinatari, interni e/o esterni al Consorzio, non direttamente interessati al tema o, comunque, non coinvolti nella trattazione del tema in oggetto.

In particolare, tale aspetto dovrà essere curato con massima attenzione nell'invio di documenti contraddistinti dalle diciture "*riservato*" o "*strettamente riservato*" o analoghe. Il Lavoratore deve inoltre aver cura di inviare o inoltrare tali comunicazioni mediante la protezione dei file a mezzo password, da comunicare esclusivamente al destinatario tramite mezzo differente rispetto a quello dell'invio (es. attraverso invio di sms o di successiva separata e-mail).

n) È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario.

o) È obbligatorio porre la massima attenzione nell'aprire i file allegati di posta elettronica prima del loro utilizzo, nonché nel verificare l'attendibilità dei messaggi ricevuti ovvero del mittente degli stessi, al fine di evitare casi di phishing o frodi informatiche.

## Assenze programmate e non programmate

Al fine di una continuità operativa, in assenza del lavoratore, si dovranno adottare i seguenti accorgimenti:

- a ciascun lavoratore, tramite apposite funzionalità di sistema, sarà offerta la possibilità di inviare automaticamente, in caso di assenze, anche improvvisa, (ad es., per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti i riferimenti di contatto (elettronici o telefonici) di un collega o altre utili modalità di contatto della struttura, oppure indicando un indirizzo di mail alternativo preferibilmente di tipo collettivo, tipo ufficio…@Consorzio.it;
- in caso di eventuali assenze non programmate (ad esempio per malattia), qualora il lavoratore non possa attivare la funzionalità suddetta (anche avvalendosi di servizi webmail) e perdurando l´assenza oltre un determinato limite temporale, il CONSORZIO potrà disporre lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (ad es., l´amministratore di sistema oppure, se presente, un incaricato del CONSORZIO per la protezione dei dati), l´attivazione di un analogo accorgimento di cui al punto precedente, avvertendo gli interessati;
- qualora, in caso di assenza improvvisa o prolungata e improrogabili, il CONSORZIO, per necessità legate all´attività lavorativa, debba conoscere il contenuto dei messaggi di posta elettronica, l´interessato potrà delegare, mediante apposito modulo, un altro lavoratore (fiduciario) che provvederà a verificare il contenuto di messaggi ricevuti inviando al Responsabile dell'Unità di appartenenza solo quelli ritenuti rilevanti per lo svolgimento dell´attività lavorativa.

### Cessazione del rapporto di lavoro

In caso di cessazione del rapporto di lavoro, in conformità ai principi in materia di protezione dei dati personali, il datore di lavoro, provvederà a rimuovere gli account di posta elettronica aziendale riconducibili a persone identificate o identificabili, nei tempi e nei modi di seguito illustrati:

- l'account del lavoratore verrà immediatamente disattivato con contestuale attivazione di un messaggio di risposta automatico volto ad informare i terzi della possibilità di contattare altri e diversi indirizzi e-mail, per esigenze di continuità dell'attività svolta per un tempo proporzionato con le esigenze della stessa;
- le misure tecnologiche ed organizzative adottate consentiranno di contemperare l'interesse del titolare ad accedere alle informazioni necessarie all'efficiente gestione della propria attività e a garantirne la continuità con la legittima aspettativa di riservatezza sulla corrispondenza da parte di dipendenti/collaboratori nonché dei terzi;
- gli account nominativi di posta elettronica verranno disattivati nei termini minimi richiesti per la predisposizione di quanto sopra e i contenuti saranno cancellati decorsi 30gg e comunque entro tre mesi dalla data di cessazione del rapporto di lavoro, salvo che vi siano elementi che inducano il CONSORZIO a ritenere necessario un periodo di conservazione più lungo (ad esempio, per finalità di difesa di un diritto in sede giudiziaria). Entro 30gg dalla cessazione del rapporto di lavoro il lavoratore potrà richiedere copia di mail strettamente personali;
- l'account dell'ex dipendente verrà cancellato in un tempo definito e ragionevole, come richiesto dal Garante che ha indicato un termine massimo di tre mesi
- dal giorno della cessazione del rapporto di lavoro, l'ex dipendente che cercasse di accedere o accede alla sua casella di posta, commetterebbe un illecito passibile di denuncia per accesso abusivo a sistema informatico ai sensi dell'art. 615 ter c.p. secondo cui "*Chiunque abusivamente*

*si introduce in un sistema informatico o telematico protetto da misure di sicurezza […] è punito con la reclusione sino a tre anni*".

**Controlli sulla posta elettronica**

l datore di lavoro qualora da controlli preliminari e casuali su dati anonimi o aggregati, che si riferiscano all'intera struttura aziendale o ad alcune delle sue aree, o a seguito di segnalazioni puntuali e dettagliate ravvisi anomalie, potrà procedere con controlli nominativi o su singoli dispositivi e postazioni, avvisando preventivamente il lavoratore, ad eccezione del caso in cui sussistano particolari circostanze. In nessun caso potranno essere compiuti controlli sistematici, ossia prolungati, costanti e indiscriminati.

I controlli sulla casella di posta elettronica assegnata al lavoratore potranno essere legittimamente esercitati in ragione di tutela del patrimonio aziendale, verificare la funzionalità dell'account e testarne la sicurezza, per controlli difensivi in senso stretto o per necessità di esercitare un diritto in sede giudiziale finalizzato ad accertare precise condotte illecite.

Infine, si informa che in alcuni casi particolari, su esplicita richiesta delle Autorità competenti (Guardia di Finanza, Autorità Giudiziaria, ecc.), le e-mail memorizzate nei server del CONSORZIO potrebbero essere eventualmente rese note e consegnate alle stesse per finalità di indagine.

## II. Navigazione in Internet

a) I computer aziendali abilitati alla navigazione in Internet costituiscono strumenti aziendali utilizzabili esclusivamente per lo svolgimento della propria attività lavorativa.

b) È proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

   A titolo puramente esemplificativo, e salvi i casi strettamente legati all'attività lavorativa, il Lavoratore non può utilizzare internet per:

   - upload o download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http (filmati, incontri sportivi, musica, etc.)
   - effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili
   - ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa
   - partecipazione a forum non professionali, utilizzo di chat line, bacheche elettroniche e registrazioni in guest books anche utilizzando pseudonimi o nicknames

c) Il Consorzio si riserva la facoltà di disattivare il sistema di navigazione per attività e finalità personali, nonché di "bloccare" i siti internet ritenuti non attinenti all'attività professionale,

d) Gli eventuali controlli, compiuti dal personale incaricato del servizio IT, potranno avvenire in conformità di quanto specificato nel presente Regolamento, solo a campione e periodicamente, mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi verranno conservati

non oltre 180 giorni, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza del Consorzio.

## 8. SOCIAL NETWORK

a) L'accesso a social network in orario di servizio è consentito solo se previamente previsto e autorizzato.

b) È vietata la partecipazione in orario lavorativo per motivi non professionali a forum, l'utilizzo di chat line, le registrazioni in guest book anche utilizzando pseudonimi. I Lavoratori che accedono a social network durante l'orario e sul posto di lavoro danneggiano la prestazione contrattualmente dovuta poiché sottraggono tempo all'attività lavorativa e possono altresì provocare problemi di sicurezza al sistema informatico dell'Ente.

c) In ogni caso – anche fuori dall'ambiente e/o orario di servizio - i Lavoratori devono astenersi dal pubblicare su social network notizie, commenti e/o immagini che per il loro contenuto possono ledere l'immagine e reputazione dell'Ente ovvero dei colleghi e/o superiori del Consorzio. A tale proposito si rileva che l'uso di espressioni denigratorie e lesive della reputazione del datore di lavoro e/o colleghi su social network ravvisa gli estremi della diffamazione in ragione del contesto pubblico, della conoscenza da parte di più persone e della possibile incontrollata diffusione tra i partecipanti alla rete del social network.

d) Il Consorzio si riserva di effettuare controlli a campione sui social network per verificare eventuali violazioni alle direttive qui impartite ovvero ad accordi di riservatezza.

## 9. CHAT AZIENDALI

Le chat aziendali sono destinate alle comunicazioni di servizio ai dipendenti e costituiscono strumenti di lavoro. Vanno pertanto evitati messaggi di natura personale o ludica, inclusi auguri, saluti e pubblicazioni di foto non inerenti all'attività lavorativa.

## 10. PROTEZIONE ANTIVIRUS

a) Il sistema informatico del CONSORZIO è protetto da software antivirus aggiornato quotidianamente. Ognuno deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.

b) Nel caso in cui il software antivirus rilevasse la presenza di un virus, va sospesa immediatamente ogni elaborazione in corso senza spegnere il computer, avendo cura di scollegare il PC dalla rete e segnalare prontamente l'accaduto al Responsabile IT.

## 11. ACCESSO AI DATI TRATTATI DAL LAVORATORE - SISTEMI DI CONTROLLO

a) Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, ecc.) o per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, ecc.), è facoltà della

Direzione dell'Ente, tramite il personale del servizio IT, accedere direttamente, nel rispetto della normativa vigente in materia di trattamento e protezione dei dati personali, a tutti gli strumenti informatici aziendali ed ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

Tali controlli potranno avvenire anche attraverso sistemi quali, ad esempio, firewall che consentano la creazione di black-list, blocchi e filtri, e mediante verifica dei file log presenti sui singoli device-client, al fine di effettuare la verifica di condotte illecite o di anomalie di sistema.

b) Tali attività di controllo saranno svolte in forma automatizzata e/o manuale, con modalità e strumenti volti a garantire la massima sicurezza e riservatezza degli strumenti e delle informazioni negli stessi contenuti, nonché mediante l'utilizzo di sistemi in grado di verificare in particolare i tempi di navigazione e il numero di accessi ad Internet.

c) Il controllo con i sistemi sopra descritti verrà effettuato sulla base di informazioni anonime ed aggregate, fatta salva la facoltà di procedere ad un intervento maggiormente invasivo solo qualora specifiche circostanze oggettive e documentate ne giustifichino la necessità, ovvero in caso di successive ulteriori anomalie. Gli eventuali dati trattati verranno conservati per il tempo indispensabile al corretto perseguimento delle finalità organizzative e di sicurezza del Consorzio.

d) In nessun caso i suddetti accessi potranno essere ricondotti al controllo dell'attività lavorativa ai sensi di quanto previsto dall'art. 4 Legge 300/70 (Statuto dei Lavoratori).

## 12. DIVIETO DI REGISTRAZIONE

Le riunioni interne fra colleghi devono favorire una comunicazione trasparente e libera, che possa fare emergere obiezioni e/o criticità, nel rispetto della riservatezza.

La normativa in materia di privacy consente la registrazione di conversazioni solo previo esplicito consenso di tutti i partecipanti, lettura di apposita informativa e conferimento dell'incarico al trattamento dei dati in capo al soggetto deputato alla registrazione

## 13. DATA BREACH

Il Regolamento UE n. 679/16 ha introdotto l'obbligo di notificazione (entro 72 ore) all'Autorità Garante Privacy, e talora anche di comunicazione agli interessati, nei casi in cui – a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi (es. incendi o calamità), furto e/o perdita di strumenti quali pc, cellulare, tablet, ecc.– si verifichi un rischio di perdita, distruzione o diffusione indebita di dati personali conservati, trasmessi o comunque trattati. Il mancato o ritardato adempimento della notificazione/comunicazione espone alla possibilità di irrogazione di sanzioni amministrative.

Al fine di permettere al Consorzio di provvedere alla valutazione dei rischi per i diritti e libertà delle persone fisiche e agli adempimenti suddetti nei termini di legge, è obbligatoria l'immediata segnalazione scritta al Responsabile IT (*amedeo.bacci@cbaltovaldarno.it)* di situazioni che possano comportare pericoli per i dati personali trattati: nel messaggio deve essere riportato quale oggetto "*ALERT DATA BREACH*", deve essere descritto l'evento, le possibili conseguenze, la natura dei dati violati e il loro numero almeno approssimativo, la categoria degli interessati, le misure adottate nell'immediato per porvi rimedio o attenuarne le conseguenze negative, i propri riferimenti.

Dovrà essere tenuta traccia dell'evento e dell'analisi del rischio per valutare la necessità della notificazione/comunicazione e futura consultazione e verifica.

In difetto, il responsabile della omessa tempestiva segnalazione potrà essere chiamato a rispondere dei danni subiti dal Consorzio, salve le ulteriori conseguenze disciplinari.

## 14. UTILIZZABILITA' IN GIUDIZIO

La violazione delle regole prescritte nel presente Regolamento o comunque il compimento di illeciti da parte del Lavoratore per tramite di strumenti aziendali comporterà la facoltà del Consorzio, con accertamento tramite indagine interna, di avvalersene come strumenti di prova in caso di contenzioso, con facoltà della relativa produzione in giudizio nei limiti di quanto effettivamente necessario ed utile alla propria difesa e all'assolvimento del proprio onere probatorio.

## 15. DIRITTO ALLA DISCONESSIONE E RISPETTO DELLA VITA PRIVATA

a) Al di fuori dell'orario contrattuale di lavoro, e perciò durante il riposo giornaliero e settimanale, le festività e le ferie, il Lavoratore ha diritto a disconnettersi dagli strumenti tecnologici, perciò a disattivare i dispositivi (pc, tablet, telefono) o comunque a non rispondere alle e-mail, ai messaggi o alle telefonate, salvo che particolari situazioni di urgenza o la posizione apicale del Lavoratore richiedano la sua reperibilità;

b) I Lavoratori e in particolare i Responsabili sono invitati ad usare la tecnologia e gli strumenti di comunicazione informatici in modo appropriato, per evitare ogni forma di invasione nella vita privata dei Colleghi; pertanto, si raccomanda di evitare l'abuso di telefonate, mail, messaggi (sms, chat, ecc.) al di fuori dell'orario lavorativo e durante il riposo, le ferie, la malattia, salvo comprovate urgenti necessità.

## 16. COMPORTAMENTO NEL RISPETTO DELLA PRIVACY

a) L'eventuale accesso a documenti aziendali, di qualsiasi natura, da parte di terzi deve essere richiesto per iscritto e motivato, per verificarne la legittimazione.
Qualora il Lavoratore riceva richiesta solo verbale di fornire informazioni, atti, documenti non accessibili al pubblico, dovrà informare il richiedente dei motivi che ostano l'accoglimento della richiesta, e suggerire di inoltrare motivata richiesta scritta al Responsabile di Area.

b) Nel trattare i dati personali, nell'ambito dello svolgimento delle mansioni affidate, il Lavoratore è tenuto a rispettare i principi di riservatezza, correttezza, liceità e trasparenza richiesti dal GDPR e dal D. Lgs. n. 101/2018, nonché attenersi alle istruzioni (policy, regolamenti, ecc.) impartite dal CONSORZIO, quale Titolare del trattamento.

## 17. REFERENTI IN MATERIA DI STRUMENTI INFORMATICI

**Responsabile (interno) IT :** Amedeo Bacci, tel. 3476158630, mail amedeo.bacci@cbaltovaldarno.it

**Servizio (esterno) IT:** Luca Salvietti, tel. 335369436, mail l.salvietti@ingeinformatica.it

## 18. MODIFICHE ED INTEGRAZIONI

Il Consorzio si riserva il diritto di modificare e/o integrare il presente Regolamento. Le nuove norme saranno efficaci dal momento in cui saranno comunicate ai Lavoratori

Il presente Regolamento, approvato con deliberazione dell'Assemblea n° … del 18/03/2025 entrerà in vigore dal 19/03/2025

Addì, 18/03/2025