REGOLAMENTO INFORMATICO INTERNO

INDICE

1. REVISIONI

Indice delle revisioni

Rev	Data	Descrizione	Verificato	Approvato
1	**06/09/2019**	**Prima versione**		
2	**09/12/2019**	**Seconda Versione**		

2. SCOPO

Il presente regolamento ha lo scopo disciplinare e di formare gli operatori all'utilizzo delle apparecchiature informatiche di , in riferimento alle linee guida del Garante della Privacy e relativa conformità dell'Ente Consorzio 2 AltoValdarno, al Regolamento (UE) 2016/679.

3. CAMPO DI APPLICAZIONE

Il ***"Regolamento informatico interno"*** definisce regole e gli standard di comportamento degli utilizzatori della strumentazione informatica del Consorzio 2 AltoValdarno.

nei confronti dei colleghi che fanno parte della nostra organizzazione, dei collaboratori esterni, dei clienti, dei fornitori, degli utenti.

Il ***"Regolamento informatico interno"*** deve essere conosciuto ed applicato da tutti coloro che interagiscono con la strumentazione informatica e dati in essi contenuti del nostro Ente ed in particolare:

- Il personale dipendente
- I collaboratori esterni
- Coloro che per motivi vari si trovano anche temporaneamente ad operare all'interno della nostra sede.

4. RIFERIMENTI NORMATIVI

- Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali"
- GDPR 2016/679 (Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche in materia di trattamento dei dati personali e alla libera circolazione di tali dati e che abroga la Direttiva 95/46 / CE) e relative linee guida emanate dal garante della privacy.
- Le linee guida del Garante per posta elettronica e internet pubblicato sulla Gazzetta Ufficiale n. 58 del 10 marzo 2007

5. UTILIZZO DELLE ATTREZZATURE / IMPIANTI E APPARECCHIATURE INFORMATICHE E SISTEMI DI COMUNICAZIONE.

5.1 SCRIVANIA E POSTI DI LAVORO

Ogni utente è tenuto a conservare con la massima cura tutto il materiale informatico e documentale che gli è stato affidato. Ogni utente deve tenere in ordine la propria scrivania e gli armadi evitando di tenere in vista documenti con dati sensibili e monitor in cui compaiono dati sensibili. Deve accertarsi che, ogni qualvolta lascia il posto di lavoro, in particolare durante l'intervallo di pranzo e la sera, la propria postazione informatica non sia accessibile e che il monitor sia spento.

E' fatto divieto di lasciare documenti incustoditi nelle stampanti, fotocopiatrici, duplicatori, scanner ecc.…

Se per motivi di organizzativi o espletamento di attività lavorative, l'utente si sposta dalla propria postazione di lavoro per un periodo prolungato o utilizza un'altra postazione, deve comunicarlo ed essere autorizzato dal proprio caposettore o dal suo diretto responsabile.

5.2 PREMESSA PER UTILIZZO SISTEMI INFORMATICI

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer, espone il "CONSORZIO 2 ALTO VALDARNO" a rischi di "DATA BREACH"*, creando problemi alla sicurezza e all'immagine dell'Ente stesso.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche del nostro Ente deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, il "CONSORZIO 2 ALTO VALDARNO" ha adottato un Regolamento informatico interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.

> * Per " data breach " si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dal titolare.

5.3 UTILIZZO DEL PERSONAL COMPUTER / NOTEBOOK (CLIENT)

Il Client affidato al dipendente/sede/ufficio è uno strumento di lavoro.

E' vietato ogni utilizzo non inerente all'attività lavorativa, in quanto può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L'accesso all'elaboratore è protetto da password che deve essere custodita dall'utente con la massima diligenza e non divulgata. La stessa password deve essere utilizzata per l'accesso, dopo l'attivazione dello screen saver o sospensione del sistema.

In ogni Client è configurato un Account Master il quale ha la facoltà in qualunque momento di accedere ai dati trattati da ciascun utente/operatore, ivi compresi gli archivi di posta elettronica interna ed esterna e i dati informatici contenuti.

Le credenziali di accesso dell'account master , sono custodite dal RESPONSABILE del Trattamento dei dati o dal TITOLARE del trattamento, che potrà accedere ai dati ed agli strumenti informatici esclusivamente per garantire l'operatività , la sicurezza dei sistemi ed il normale svolgimento dell'attività dell'Ente stesso, nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio in caso di prolungata assenza o impedimento dell'utente , informando tempestivamente l'utente dell'intervento di accesso realizzato.

Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione esplicita del proprio caposettore o diretto responsabile, in quanto sussiste il grave pericolo di portare Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente, autorizzati da "CONSORZIO 2 ALTO VALDARNO" tramite le figure preposte. L'inosservanza di questa disposizione, infatti, oltre al rischio di

danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'associazione 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.

Non è consentito all'utente modificare le caratteristiche impostate sul proprio Client, salvo previa autorizzazione esplicita del Capo settore o diretto Responsabile.

Il Client deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. Lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. Se l'apparato non può essere spento per qualsiasi motivo, l'operatore deve attivare lo screen saver con riattivazione sotto password o disconnettersi dal sistema.

Non è consentita l'installazione e utilizzo di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio dispositivi di archiviazione USB, masterizzatori, modem, …), se non con l'autorizzazione espressa della Capo settore o diretto Responsabile.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna non autorizzati, avvertendo immediatamente il responsabile del trattamento dei dati o il proprio Capo settore o diretto Responsabile.

5.4 UTILIZZO E ACCESSO AGLI ARCHIVI COMUNI, DATI CENTRALIZZATI E UNITA' DI RETE CENTRALIZZATE

E' consentito l'utilizzo e accesso ai dati e unità sopra citate solo previa autorizzazione diretta del proprio Capo settore o diretto Responsabile, i quali hanno il compito di organizzare, ciascuno per il proprio settore di riferimento, le cartelle/file contenuti in queste unità definendone le autorizzazioni a livello di account di dominio. Questa attività può essere svolta anche con l'ausilio/consulenza di figure esterne.

L'account a livello di dominio aziendale informatico, viene creato all'inizio del rapporto lavorativo e cesserà alla conclusione di tale rapporto.

L'utilizzo ed accesso a questi dati è consentito solo per attività lavorativa riconducibile all'Ente e alla figura dell'utente.

E' consentito lo spostamento del dato/file/cartella nel proprio client solo per lo svolgimento delle attività lavorative autorizzate e una volta terminata la stessa il dato/file/cartella deve essere ricollocato nell'unità informatica di provenienza.

Non è assolutamente consentita la conservazione oltre il tempo strettamente necessario all'espletamento dell'attività, del dato/file/cartella , nel proprio client o altra apparecchiatura informatica al di fuori di quelle centralizzate autorizzate.

La conservazione o copie di dati provenienti da archivi informatici centralizzati dell'Ente deve essere espressamente autorizzata e motivata dal Capo settore di riferimento o diretto Responsabile.

I dati contenuti in archivi CLOUD (quindi su hardware esterno all'Ente) sono ugualmente sottoposti al presente regolamento e devono essere trattati/utilizzati nel rispetto della normativa GDPR e delle norme previste dai singoli fornitori.

5.5 UTILIZZO DELLA RETE

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup.

Le password d'ingresso alla rete ed ai programmi sono segrete e personali. È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente e password.

Il Consorzio 2 Alto Valdarno, tramite le figure preposte, può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui Client sia sulle unità di rete, dopo avere informato e ricevuto autorizzazione dal Responsabile del Trattamento (Caposettore o Direzione).

Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili, sia lato Client sia lato unità di rete centralizzate (Server, NAS, etc…) . Particolare attenzione deve essere prestata alla duplicazione dei dati. È fatto divieto l'uso di sistemi di backup o duplicazione dati non autorizzati dal caposettore o diretto responsabile.
È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni.

5.6 CONNESSIONI ESTERNE ALLA RETE INFORMATICA INTERNA

Sono consentite connessioni esterne alla rete informatica interna solo attraverso l'utilizzo di linee sicure e monitorate (VPN etc…) da apparecchiature apposite (Firewall , etc…)
L'utente / operatore che si connette dall'esterno è sottoposto alle stesse indicazioni presenti in questo regolamento informatico.
Non è consentito l'utilizzo di software di connessione diretta agli apparati informatici interni alla rete aziendale, salvo software di teleassistenza su programmi interni all'Ente e autorizzati.
Ogni collegamento con l'esterno deve comunque essere autorizzato dai Caposettore o Direzione.

5.7 GESTIONE DELLE PASSWORD

Le password di accesso ai dispositivi informatici, alla rete, ai programmi e alle cartelle condivise devono essere modificate, a cura dell'utente autorizzato, al primo utilizzo e, successivamente, almeno ogni sei mesi; nel caso di trattamento di dati sensibili e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi.
Le password possono essere formate da lettere (maiuscole o minuscole) ,numeri e devono essere composte da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'utilizzatore.
La password deve essere immediatamente sostituita, dandone comunicazione al Capo settore o diretto Responsabile, nel caso si sospetti che la stessa abbia perso la segretezza.
La password è strettamente personale e non deve essere a conoscenza di altri utenti o figure interne ed esterne all'Ente.
Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia al Responsabile del trattamento/Capo settore/diretto Responsabile.
In nessun caso devono essere annotate password in chiaro sia su supporto cartaceo che informatico e non devono essere salvate all'interno dei browser di ricerca.

5.8 UTILIZZO DEI SUPPORTI MAGNETICI / STORAGE / CHIAVI USB

L'eventuale utilizzo dei supporti sopra citati contenenti dati sensibili e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.
Queste tipologie di supporti devono essere custoditi in archivi/locali chiusi a chiave o da personale autorizzato direttamente dal proprio Capo settore o diretto Responsabile.
La presenza di questi supporti deve essere autorizzata e registrata ed il contenuto al loro interno deve essere criptografato e/o protetto da password.

5.9 UTILIZZO DEI PC PORTATILI E APPARATI MOBILI

L'utente è responsabile del PC portatile/apparato mobile assegnatogli dal CONSORZIO 2 ALTO VALDARNO e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
Ai PC portatili/apparato mobile si applicano le regole di utilizzo previste per i Client (vedi punto 5.3).
I PC portatili/apparati mobili utilizzati all'esterno (convegni, visite in azienda, ecc…), in caso di allontanamento, devono essere custoditi in un luogo protetto.

5.10 UTILIZZO POSTA ELETTRONICA

La casella di posta elettronica, assegnata dall'Ente Consorzio 2 AltoValdarno, è uno strumento di lavoro. Le persone/sede/ufficio assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

È fatto divieto di utilizzare le caselle di posta elettronica aziendale per l'invio o ricezione di messaggi personali.

È fatto divieto di utilizzare le caselle di posta elettronica aziendale per iscrizioni a servizi newsletter o mailing list senza esplicita autorizzazione del Capo settore o diretto Responsabile.

È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per il CONSORZIO 2 ALTOVALDARNO deve essere visionata e autorizzata dal Caposettore/diretto Responsabile/Direzione o in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.

La documentazione elettronica che costituisce per l'Ente "know how aziendale" protetto, e che, quindi, viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto a tutela del patrimonio dell'Ente, non può essere comunicata all'esterno senza preventiva autorizzazione del Capo settore/diretto Responsabile/Direzione.

È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti certificati come PEC o raccomandate tradizionali.

Per la trasmissione di file all'interno della rete informatica del CONSORZIO 2 ALTOVALDARNO è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati.

È obbligatorio controllare i file "attachements" di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

È vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve dare comunicazione immediata al Capo settore/diretto Responsabile/Direzione o Responsabile dei sistemi informatici.

Non si devono in alcun caso attivare gli allegati di tali messaggi o link presenti nelle stesse.

E' fatto divieti di utilizzare caselle di posta elettronica non autorizzate direttamente dall'Ente (caselle personali etc..).

5.11 USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

Il Client o apparato mobile abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal Capo settore/diretto Responsabile/Direzione. È' tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati e con il rispetto delle normali procedure di acquisto.

È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

E' vietato accedere a siti per la condivisione e lo streaming di contenuti multimediali e simili, a meno che non si tratti di siti riconducibili all'attività lavorativa.

5.12 SISTEMI ANTIVIRUS E MONITORAGGIO

Su tutte le apparecchiature informatiche presenti nei locali di CONSORZIO 2 ALTOVALDARNO o date in dotazione ad utenti/operatori esterni, sono presenti dei software antivirus. L'utilizzo di tali strumenti è reso necessario al fine di

prevenire intrusioni o furti di dati dalla rete informatica e qualora si presentasse tale situazione per permettere al Responsabile e Titolare del trattamento dati di darne immediata comunicazione agli organi preposti.
L'Ente si riserva la facoltà di utilizzare strumenti informatici Hardware/Software al fine di avere una reportistica in tempo reale attraverso il monitoraggio della rete internet / scambio dati e controllo hardware e software su tutte e di tutte le apparecchiature informatiche presenti.

5.13 UTILIZZO DEL FAX E APPARECCHIUTURE DI STAMPA

Si raccomanda di non lasciare documenti incustoditi presso le postazioni di fax e su apparecchiature di stampa all'atto di invio, copie o scansioni. Qualora il dipendente sia prossimo a ricevere atti contenenti dati o informazioni riservate via fax, avrà cura di monitorare la postazione fax e preservare – limitatamente alle oggettive possibilità – la conoscibilità di tali dati o informazioni, da parte di terzi non autorizzati.

5.14 GESTIONE, CONSERVAZIONE E CONTROLLO DEI DATI INFORMATICI

È fatto divieto utilizzare sistemi di crittografia, codificazione e simili ai dati se non con procedure e sistemi espressamente autorizzati dal CONSORZIO 2 ALTOVALDARNO.

5.15 FURTO / SMARRIMENTO APPARECCHIATURE INFORMATICHE

L'utente / utilizzatore di apparecchiature informatiche fornite dal Consorzio 2 Alto Valdarno, deve subito rendere noto ai propri superiori/responsabili l'eventuale mancanza di tali apparecchiature, evidenziando se si tratta di un furto o smarrimento, al fine di permettere alle figure preposte di procedere con una segnalazione al Garante della Privacy ed alle autorità competenti.

6. PRESCRIZIONI INTERNE E VERIFICHE/CONTROLLI

6.1 SEGRETO PROFESSIONALE

Il dipendente/collaboratore interno o esterno, in mancanza di autorizzazione dal proprio Capo settore / diretto Responsabile, non può divulgare, pubblicare o comunicare in alcun modo a terzi, direttamente o indirettamente, in toto o in parte, le informazioni apprese mediante strumenti informatici in occasione dello svolgimento delle mansioni per le quali è stato assunto dall'Ente, né potrà usarle, sfruttarle o disporne in proprio o tramite terzi.
Gli obblighi del dipendente/collaboratore previsti in questo capo non termineranno all'atto di cessazione del rapporto di lavoro, se non in riferimento a quelle specifiche parti delle informazioni che il dipendente possa dimostrare che erano già di pubblico dominio al momento della conclusione del rapporto, o che lo sono diventate in seguito per fatto a lui non imputabile.

6.2 OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY

È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicate nella lettera di designazione di incaricato del trattamento dei dati ai sensi del Regolamento (UE) 2016/679, relativo alla protezione delle persone fisiche in materia di trattamento dei dati personali e alla libera circolazione di tali dati.

6.3 CONTROLLI

Il CONSORZIO 2 ALTOVALDARNO, tramite delle figure preposte ed autorizzate, si riserva di effettuare controlli sul corretto utilizzo degli strumenti informatici e telematici nel rispetto delle normative vigenti e del presente regolamento, nonché nel rispetto dello Statuto dei Lavoratori.

I controlli verranno effettuati dal Responsabile della sicurezza/Responsabile del trattamento dati con l'ausilio dell'assistenza tecnica (interna o esterna) anche dietro segnalazione proveniente da propri operatori , da organi di polizia o da report generati dai programmi di controllo della struttura informatica.
Controlli ordinari e verifiche verranno effettuati con cadenza semestrale.

6.4 NON OSSERVANZA DELLA NORMATIVA

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

6.5 AGGIORNAMENTO E REVISIONE

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dalla Direzione.
Il presente Regolamento è soggetto a revisione con frequenza annuale.