

	Titolo del documento				
	Istruzioni Operative e Regolamento sul trattamento dei dati				
	Nr. / No.	Vers. Aziendale	Rev.	Data:	Pg.
	REG-002	0	1	10.06.2024	Pagina 1 di 7
Autore: Luca Salini		Approvato:			

Istruzioni operative e regolamento sul trattamento dati

OBIETTIVO

Il presente Regolamento si propone di stabilire modalità e finalità di utilizzo dei beni aziendali, disciplinando le condizioni per il corretto utilizzo degli strumenti informatici, telematici e telefonici da parte degli utenti di TUTOR Società consortile a responsabilità limitata ed applicabile presso le sedi di Piacenza e Fiorenzuola d'Arda.

Il regolamento, inoltre, oltre a dettare una disciplina per l'utilizzo degli strumenti informatici/telefonici aziendali, vuole costituire un utile strumento per sensibilizzare al rispetto della normativa sulla tutela legale del software e alla tutela del know-how aziendale.

CONTROLLI

Tutor, in linea con quanto prescritto dall'ordinamento giuridico italiano (art. 4, Statuto dei Lavoratori), esclude la configurabilità di forme di controllo aziendali aventi direttamente ad oggetto l'attività lavorativa dell'Utente. È comunque sempre possibile che per ragioni organizzative e produttive ovvero per esigenze dettate dalla sicurezza del lavoro o ancora per la difesa del patrimonio aziendale si utilizzino sistemi informatici, impianti o apparecchiature dai quali possano derivare controlli incidentali delle attività lavorative.

Tutor Scarl, attraverso i propri responsabili di struttura, ha facoltà di svolgere gli accertamenti necessari e adottare ogni misura atta a garantire la sicurezza e la protezione dei sistemi informatici, delle informazioni e dei dati. Le modalità di svolgimento di tali accertamenti, anche se saranno verificate le future linee guida adottate dall'Agenzia per l'Italia Digitale e Garante Privacy, al momento risultano le seguenti:

- Accesso ai sistemi con profilazione personale
- Memorizzazione dei log dei sistemi e negli applicativi, dove previsto. Tali log sono memorizzati ed utilizzati/visionati solamente in caso di necessità.
- Filtraggio del traffico internet per determinate categorie di siti (armi, pedopornografia, etc.)
- Sistemi di filtraggio della posta elettronica al fine di prevenire SPAM ed attacchi ai dipendenti di Tutor Scarl.

UTILIZZO RISORSE INFORMATICHE

Tutte le risorse informatiche e/o qualsiasi altro tipo di strumentazione di lavoro sono di esclusiva proprietà TUTOR.

L'Azienda si riserva il controllo e la gestione integrale delle risorse informatiche aziendali; è fatto divieto di installare hardware fisso o removibile (a titolo esemplificativo ma non esaustivo: supporti esterni, modem, ecc.) sulla strumentazione in uso qualora ciò non risulti espressamente richiesto ed autorizzato dall'Azienda.

L'utente deve pertanto utilizzare esclusivamente la strumentazione posta a disposizione dall'Azienda.

L'Azienda si riserva di rimuovere qualsiasi elemento hardware la cui installazione non sia stata appositamente prevista o autorizzata.

L'accesso al Personal Computer deve essere protetto da password che deve essere conosciuta e custodita dall'incaricato con la massima diligenza.

In caso di allontanamento dalla propria postazione informatica è fatto obbligo all'utente di interrompere la sessione attivando il salva-schermo protetto da password oppure eseguendo il log-out utente oppure ancora spegnendo il computer. Lasciare il dispositivo incustodito e connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne l'indebito uso.

Sui PC dotati di apparati per la riproduzione audiovisiva (scheda audio, lettore CD/DVD) non è consentito l'ascolto di programmi, files audio o musicali, se non a fini prettamente lavorativi.

Qualora si rendessero necessarie modifiche alle configurazioni impostate sul PC in uso, occorre darne comunicazione al proprio Responsabile di Sede.

	Titolo del documento				
	Istruzioni Operative e Regolamento sul trattamento dei dati				
	Nr. / No.	Vers. Aziendale	Rev.	Data:	Pg.
	REG-002	0	1	10.06.2024	Pagina 2 di 7
Autore: Luca Salini		Approvato:			

Al fine di recepire il Decreto n°81 del 2023 al dipendente è consentito l'utilizzo degli strumenti informatici forniti dall'amministrazione per poter assolvere alle incombenze personali senza doversi allontanare dalla sede di servizio, purché l'attività sia contenuta in tempi ristretti e senza alcun pregiudizio per i compiti istituzionali.

SALVATAGGIO DATI

I dati vanno salvati secondo la procedura stabilita e nelle cartelle identificate dal titolare sul server di sede. Qualsiasi file/dato estraneo all'attività lavorativa o non espressamente autorizzato, non può, nemmeno in via transitoria, essere salvato sul pc in uso all'Utente.

I dati relativi all'attività lavorativa possono anche essere memorizzati in locale sul PC/Notebook dell'utilizzatore qualora sia prevista la sincronizzazione di tali cartelle con i sistemi cloud (es: OneDrive) aziendali rilasciati dal CFP.

ACCESSO ED USO DEI SISTEMI

L'utente si connette alla rete tramite autenticazione univoca personale.

Le credenziali di autenticazione alla rete (o se l'Utente lavora in locale, di accesso al sistema operativo) devono essere custodite e preservate dalla conoscibilità di colleghi o soggetti esterni all'Azienda. In nessun caso devono essere annotate password in chiaro sia su supporto cartaceo che informatico. I requisiti minimi di complessità delle password sono riportati successivamente. Qualora l'intestatario della password ritenga che un soggetto non autorizzato possa essere venuto a conoscenza della propria password, dovrà provvedere ad attivare la procedura di sostituzione della stessa e a comunicare il fatto al proprio Responsabile di Sede.

SOFTWARE

Sul pc in uso non devono essere installati programmi che non siano ufficialmente forniti da TUTOR. È fatto divieto all'Utente sottoscrivere licenze – anche a titolo gratuito – per programmi finalizzati ad essere installati sul pc in uso del medesimo Utente. L'Azienda, peraltro, ricorda all'utilizzatore che costituiscono illecito penale le condotte consistenti nella illecita duplicazione o riproduzione di software ai sensi della legge sul diritto d'autore n. 633/41.

Eventuali esigenze di nuovi applicativi da installare sui PC dati in uso ai dipendenti, devono essere richiesti al Responsabile di Sede che provvederà ad inviare la richiesta al fornitore specifico che detiene anche la responsabilità di conteggio e fornitura delle licenze software, dove previsto.

UTILIZZO RETE LOCALE

La rete interna, istituita appositamente per permettere collegamenti funzionali tra utenti che prestano servizio all'interno della struttura lavorativa, non può esser utilizzata per scopi diversi da quelli ai quali è destinata.

Deve essere premura di ciascun utente non diffondere dati relativi a configurazioni della rete interne a terzi soggetti non espressamente autorizzati ad aver notizia di tali dati. È fatto divieto scaricare e/o memorizzare dalla rete documenti, file o dati non attinenti alle proprie mansioni lavorative.

	Titolo del documento				
	Istruzioni Operative e Regolamento sul trattamento dei dati				
	Nr. / No.	Vers. Aziendale	Rev.	Data:	Pg.
	REG-002	0	1	10.06.2024	Pagina 3 di 7
Autore: Luca Salini		Approvato:			

UTILIZZO RETE INTERNET

Per i pc con connessione internet non è consentito:

- navigare in siti non attinenti allo svolgimento delle mansioni assegnate;
- la partecipazione, per motivi non professionali, a *Forum*, l'utilizzo di *chat line*, di bacheche elettroniche e le registrazioni a servizi online anche utilizzando pseudonimi (o *nicknames*) potendo esporre a rischi di sicurezza la rete aziendale;
- utilizzare la banda disponibile per effettuare scaricamenti di file di grandi dimensioni (indicativamente di qualche Gigabyte) se non specificatamente autorizzati anche se finalizzate ad attività lavorative.
- Nelle sedi dell'ente è presente anche una rete WI-FI che risulta profilata con due reti separate al fine di rendere maggiormente sicuro lo scambio dei dati.
 - Rete WI-FI GUEST. Questa rete è dedicata agli ospiti ed ai device personali anche dei dipendenti che non devono necessariamente gestire applicativi aziendali ma hanno necessità solamente di una connessione ad Internet. La password di collegamento è fornita dalla reception di sede.
 - Rete WIFI Tutor. Questa rete è dedicata ai dispositivi aziendali di Tutor che necessitano un collegamento ai dati ed ai server contenenti i documenti/dati di lavoro. Le credenziali di accesso a tale rete sono state diffuse al personale interessato.

STRUMENTI PERSONALI

È consentito l'utilizzo di dispositivi personali (smartphone, tablet, notebook, etc.) per la consultazione della casella di posta elettronica dell'ente, anche se rimane responsabilità dell'utente avvisare il più velocemente possibile in merito a smarrimenti di dispositivi personali in cui fossero configurate le credenziali aziendali. Gli utenti sono tenuti a provvedere in autonomia (previa formazione) alla cancellazione del device personale nella piattaforma cloud della casella email qualora smarrito. In caso non fosse possibile si dovrà inviare richiesta di cancellazione del device al fornitore del sistema email.

Accesso alla VPN aziendale da dispositivi personali deve invece essere richiesta al Responsabile di Sede che a sua volta chiederà al fornitore la relativa abilitazione.

DISPOSITIVI RIMOVIBILI

Gli apparecchi di proprietà personale dell'Utente quali computer portatili, computer e smartphone non potranno essere collegati alle reti informatiche aziendali, salvo preventiva autorizzazione definita con il Responsabile di Sede che indicherà anche le contromisure da attuare, nonché chiedere al fornitore esterno l'abilitazione dove necessario.

I dispositivi USB sono permessi ma il loro utilizzo è fortemente sconsigliato in assenza di un comportamento che preservi le informazioni e i dati personali in esso contenuti.

L'utilizzo dei dispositivi USB è permesso sia per le attività di didattica (presentazioni didattiche, video didattici, etc.) sia per l'utilizzo personale.

In caso contrario, ovvero dove sono presenti dati personali o sensibili, devono essere custoditi in un luogo protetto e non accessibile (cassaforte, armadio chiuso a chiave etc.) quando non utilizzati.

Si chiede pertanto ai docenti di valutare attentamente i contenuti caricati sui dispositivi USB e quando si rende necessario utilizzarli per informazioni e dati personali delle attività didattiche occorre chiedere autorizzazione preventiva al Responsabile di Sede che indicherà anche le contromisure da attuare (Es: cifratura dei dati).

È consigliato altresì l'utilizzo delle cartelle di rete e dei cloud dell'Ente per lo scambio di tali informazioni al posto dei dispositivi USB.

In caso di smarrimento o furto occorre tempestivamente informare il Titolare ed avviare, nel caso di smarrimento di dati personali, la procedura di notifica al Garante Privacy seguendo il modello procedurale indicato nel documento PRO0021.

	Titolo del documento				
	Istruzioni Operative e Regolamento sul trattamento dei dati				
	Nr. / No.	Vers. Aziendale	Rev.	Data:	Pg.
REG-002		0	1	10.06.2024	Pagina 4 di 7
Autore:	Luca Salini		Approvato:		

GESTIONE E UTILIZZO DELLA POSTA ELETTRONICA AZIENDALE

La casella di posta elettronica assegnata all'utente è uno strumento di lavoro è quindi destinata esclusivamente all'utilizzo professionale e pertanto considerata proprietà di Tutor Scarl sia quale indirizzo email sia come contenuto dei messaggi. L'ente si ritiene pertanto autorizzato ad effettuare qualsiasi variazione si renda necessaria al sistema ed alla configurazione delle caselle e del servizio di posta elettronica senza nessuna comunicazione preventiva dell'utilizzatore.

Si fa presente inoltre che:

- (Vedi Decreto n°81 del 2023) non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica, o che costituiscano comunque condotta illecita o che siano in qualunque modo fonte di responsabilità dell'amministrazione.;
- non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, *Forum*, *newsletter* o *mail-list*, non attinenti l'attività lavorativa;
- è fatto divieto di divulgare le notizie, i dati e qualsiasi altra informazione appresa in occasione della ricezione o invio di posta elettronica, in quanto coperte dal segreto professionale cui sono tenuti i dipendenti in ottemperanza agli obblighi di fedeltà e correttezza;
- la posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei e, dunque, è preferibile non usarla per inviare documenti di lavoro "Strettamente Riservati" o qualsiasi documento che non sia pubblicamente distribuibile a meno di proteggere i file con protezioni aggiuntive (Es: File .zip con password comunicata su altro canale o link a documenti del server o OneDrive aziendale);
- in caso di assenza prolungata, sarà attivata dal gestore la risposta automatica di assenza con indicazioni per il rinvio verso caselle presidiate. Se necessario ai fini dell'attività dell'Ente, verrà effettuato l'accesso alla casella da parte di personale autorizzato previa notifica all'intestatario del profilo stesso. Tale casella verrà rimessa in sicurezza con un reset delle password al momento della ripresa dell'attività da parte del dipendente;
- è fatto divieto di divulgare le notizie, i dati e qualsiasi altra informazione appresa in occasione della ricezione o invio di posta elettronica, in quanto coperte dal segreto professionale cui sono tenuti gli Utenti in ottemperanza agli obblighi di fedeltà e correttezza;
- è buona norma rispondere ad e-mail pervenute solo da mittenti conosciuti e cancellare preventivamente le altre;
- non è consigliabile collegarsi a siti internet contenuti all'interno di messaggi: occorre controllare attentamente gli allegati di posta elettronica o i link richiamati nella mail prima del loro utilizzo per evitare possibili attacchi di phishing;
- In caso di dubbi o perplessità su mittenti, allegati o link che possano sembrare "sospetti" si consiglia di rivolgersi ai Responsabili di Sede che se necessario coinvolgeranno i fornitori esterni pertinenti.

In caso di interruzione del rapporto di lavoro con l'Utente, l'indirizzo di posta elettronica vedrà un reset della password il giorno di cessazione del rapporto di lavoro. Passati 15 giorni dalla data di cessazione del dipendente la casella può prevedere:

- Disabilitazione e cancellazione definitiva della casella email.
- Trasferimento ad altro dipendente tramite cambio dello username e riutilizzo della licenza software.

È sconsigliato, a meno di esigenze specifiche che garantiscano la continuità operativa della sede, effettuare redirect delle email ad altri dipendenti.

Come da decreto n°81 del 2023 l'utilizzo di account istituzionali è consentito per i soli fini connessi all'attività lavorativa o ad essa riconducibili e non può in alcun modo compromettere la sicurezza o la reputazione dell'amministrazione.

	Titolo del documento				
	Istruzioni Operative e Regolamento sul trattamento dei dati				
	Nr. / No.	Vers. Aziendale	Rev.	Data:	Pg.
REG-002		0	1	10.06.2024	Pagina 5 di 7
Autore:	Luca Salini		Approvato:		

L'utilizzo di caselle di posta elettronica personali è di norma evitato per attività o comunicazioni afferenti il servizio, salvi i casi di forza maggiore dovuti a circostanze in cui il dipendente, per qualsiasi ragione, non possa accedere all'account istituzionale.

Il dipendente è responsabile del contenuto dei messaggi inviati. I dipendenti si uniformano alle modalità di firma dei messaggi di posta elettronica di servizio individuate dall'amministrazione di appartenenza. Ciascun messaggio in uscita deve consentire l'identificazione del dipendente mittente e deve indicare un recapito istituzionale al quale il medesimo è reperibile.

Gestioni delle credenziali di autenticazione

L'accesso dati personali è consentito alle persone in possesso di "credenziali di autenticazione" che permettono il superamento di una procedura di autenticazione. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'Incaricato (user-id) associato ad una parola chiave riservata (password).

Le credenziali di autenticazione sono assolutamente personali e non cedibili, per nessuna ragione. Non vanno mai condivise con altri utenti, anche se anch'essi autorizzati al trattamento.

Utilizzo di Password Robusta (Policy Password)

Per impostare le nuove password ogni 90 giorni occorre rispettare le seguenti regole:

Usare almeno 8 caratteri.

Usare lettere, numeri e almeno un carattere tra . ; \$! @ - > <

Non utilizzare le 3 password precedenti

Non utilizzare date di nascita, nomi o cognomi propri o di parenti o nomi di vocabolario.

Non sceglierla uguale alla matricola o alla user-id

Custodirla sempre in un luogo sicuro e non accessibile a terzi (es: Memorizzandola a mente o utilizzando tool di gestione sicura delle password secondo le regole aziendali).

In caso di utilizzo di 10 password errate l'utenza verrà bloccata e sarà necessario rivolgersi al Responsabile di sede che riporterà la richiesta al fornitore di gestione del dominio interno per la reimpostazione della password.

ISTRUZIONI DA SEGUIRE DURANTE UNA SESSIONE DI LAVORO.

Non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento. È necessario terminare la sessione di lavoro ogni volta che ci si deve allontanare dalla postazione lasciandola incustodita effettuando un log out o mettendo in atto altri accorgimenti come il blocco automatico dopo un certo periodo di inattività.

GESTIONE CONSERVAZIONE E CONTROLLO DEI DATI INFORMATICI

È fatto divieto applicare sistemi di crittografia, codificazione e simili ai dati se non espressamente richiesto dall'Ente secondo la tipologia di dato o documento.

GESTIONE FOTOGRAFIE / VIDEO / IMMAGINI

Siete pregati di porre attenzione particolare a foto o immagini scattate durante eventi o uscite. È vietata la divulgazione non autorizzata.

	Titolo del documento				
	Istruzioni Operative e Regolamento sul trattamento dei dati				
	Nr. / No.	Vers. Aziendale	Rev.	Data:	Pg.
REG-002		0	1	10.06.2024	Pagina 6 di 7
Autore: Luca Salini		Approvato:			

GESTIONE DEI SOCIAL MEDIA (Decreto n°81 nel 2023)

Nell'utilizzo dei propri account di social media, il dipendente utilizza ogni cautela affinché le proprie opinioni o i propri giudizi su eventi, cose o persone, non siano in alcun modo attribuibili direttamente alla pubblica amministrazione di appartenenza.

In ogni caso il dipendente è tenuto ad astenersi da qualsiasi intervento o commento che possa nuocere al prestigio, al decoro o all'immagine dell'amministrazione di appartenenza o della pubblica amministrazione in generale.

Al fine di garantirne i necessari profili di riservatezza le comunicazioni, afferenti direttamente o indirettamente il servizio non si svolgono, di norma, attraverso conversazioni pubbliche mediante l'utilizzo di piattaforme digitali o social media. Sono escluse da tale limitazione le attività o le comunicazioni per le quali l'utilizzo dei social media risponde ad una esigenza di carattere istituzionale.

Al momento Tutor Scarl non ha definito una "social media policy" ma si riserva la possibilità di realizzarla in futuro.

Fermi restando i casi di divieto previsti dalla legge, i dipendenti non possono divulgare o diffondere per ragioni estranee al loro rapporto di lavoro con l'amministrazione e in difformità alle disposizioni di cui al decreto legislativo 13 marzo 2013, n. 33, e alla legge 7 agosto 1990, n. 241, documenti, anche istruttori, e informazioni di cui essi abbiano la disponibilità.»;

GESTIONE DOCUMENTI CARTACEI

TRATTAMENTO SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Per il trattamento dei documenti cartacei rispettare sempre le indicazioni del Titolare in merito agli archivi a cui poter accedere e ai documenti che è possibile trattare: non trattare nessun documento al di fuori delle autorizzazioni.

Una volta presi in carico, gli atti e i documenti, contenenti dati personali, non devono essere lasciati liberi di vagare senza controllo ed a tempo indefinito per gli uffici, ma occorre provvedere in qualche modo a controllarli e custodirli, per poi restituirli al termine delle operazioni affidate. Le misure di sicurezza applicate alle copie o alle riproduzioni dei documenti contenenti dati personali devono essere identiche a quelle applicate agli originali.

Custodia

I documenti contenenti dati personali devono essere custoditi in modo da non essere accessibili a persone non autorizzate al trattamento (es. armadi o cassette chiusi a chiave).

I documenti contenenti dati personali che vengono prelevati dagli archivi per l'attività quotidiana devono esservi riposti a fine giornata.

I documenti contenenti dati personali non devono rimanere incustoditi su scrivanie o tavoli di lavoro.

I documenti contenenti dati particolari, sensibili o giudiziari (es: Stato di salute, convinzioni politiche, religiose, sindacali, etc..) devono essere custoditi in armadi chiusi a chiave.

Comunicazione

la condivisione, la comunicazione e l'invio di documenti contenenti dati personali, deve avvenire solo verso persone che ne necessitano per lo svolgimento delle proprie mansioni lavorative e quindi espressamente autorizzate dal titolare del trattamento. I dati non devono essere comunicati all'esterno dell'organizzazione, ad eccezione dei soggetti espressamente previsti.

Distruzione

Qualora sia necessario distruggere i documenti contenenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere sminuzzati in modo da non essere più ricomponibili.

	Titolo del documento				
	Istruzioni Operative e Regolamento sul trattamento dei dati				
	Nr. / No.	Vers. Aziendale	Rev.	Data:	Pg.
	REG-002	0	1	10.06.2024	Pagina 7 di 7
Autore:	Luca Salini		Approvato:		

RISERVATEZZA DEI DATI

Per "Informazioni Riservate" si intendono tutte le informazioni di qualsivoglia natura riferite od apprese in occasione dello svolgimento delle mansioni lavorative. Il dipendente stesso si impegna a non comunicarle e/o divulgarle se non per ragioni connesse all'attività lavorativa e comunque nel rispetto della vigente normativa sulla protezione dei dati personali e ad adottare tutte le misure ragionevolmente necessarie per non pregiudicarne la riservatezza. Il dipendente si impegna ad utilizzare le Informazioni Riservate unicamente allo scopo di effettuare l'attività lavorativa cui è preposto e di conseguenza a non usare tali informazioni per altre finalità e/o in maniera tale che dalla diffusione delle stesse possa derivare un qualsiasi danno a TUTOR.

CONCLUSIONI

Per qualsiasi dubbio relativo all'applicazione pratica o all'interpretazione del presente regolamento, il dipendente può rivolgersi al proprio Responsabile di Sede.
Qualora al presente regolamento TUTOR intenda apporre modifiche, queste saranno applicate dandone conoscenza immediata al dipendente.

Piacenza, 10 Giugno 2024

TUTOR, in persona del delegato dal rappresentante legale ____Dott. Mirco Potami____