REGOLAMENTO INTERNO IN MATERIA DI RISERVATEZZA DEI DATI PERSONALI E SICUREZZA DEI SISTEMI INFORMATIVI AZIENDALI

Art. 1 PREMESSA.
Il presente regolamento intende formalizzare alcune linee guida per garantire il rispetto della vigente normativa in materia di riservatezza dei dati personali e di sicurezza dei sistemi informativi rispetto ai rischi distruzione o perdita delle informazioni, accesso non autorizzato e trattamento non consentito.

Il comportamento degli operatori dovrà essere conformato alle misure di sicurezza di seguito stabilite dall'Ente, ai sensi del GDPR 2016/679 e del Codice della Privacy.

Conformare il proprio comportamento a quanto di seguito indicato contribuirà al raggiungimento degli obiettivi della sicurezza, riassumibili nei tre aspetti distinti:

- **Disponibilità**: ovvero, garantire l'accesso alle informazioni e ai servizi di rete da parte del personale incaricato in relazione alle esigenze lavorative;
- **Riservatezza**: ovvero, garantire la prevenzione di accessi abusivi o non autorizzati alle informazioni, ai servizi e ai sistemi;
- **Integrità**: ovvero, garantire che le informazioni non siano state alterate da incidenti o abusi.

Il raggiungimento di questi obiettivi richiede non solo l'utilizzo di appropriati strumenti tecnologici, ma anche gli **opportuni meccanismi organizzativi**; infatti, le misure tecniche, per quanto sofisticate, non saranno efficienti se non utilizzate propriamente.

In particolare, le precauzioni di tipo tecnico/informatico possono proteggere le informazioni durante il loro transito attraverso i sistemi ed anche quando queste sono registrate su un disco fisso di un elaboratore, ma nel momento in cui esse raggiungono l'utente incaricato, la loro protezione dipende esclusivamente dall'operato di quest'ultimo e nessuno strumento tecnologico può sostituirsi al suo **senso di responsabilit**à e **al rispetto di alcune semplici norme di comportamento** e all'**obbligo di riservatezza dei dati trattati**.

Art. 2 AMBITO DI APPLICAZIONE
I principi disciplinati dal presente documento si applicano al trattamento di dati personali nello svolgimento di mansioni lavorative da parte di lavoratori con rapporto di subordinazione, di collaboratori e di terzi soggetti espressamente autorizzati.

Titolare del trattamento è il Consorzio Universitario Piceno che si avvale dell'Amministratore di sistema per le finalità di cui al presente Regolamento

Art. 3 RESPONSABILITÀ DI ATTUAZIONE
Tutto il personale, in funzione del proprio ruolo e delle proprie competenze, è responsabile dell'applicazione del presente regolamento.

Tutto il personale, inoltre, è responsabile della vigilanza in merito alla corretta attuazione del presente regolamento.

Art. 4 DISTRIBUZIONE
Il presente Regolamento ha come destinatari tutti gli utenti del sistema informativo e gli utenti che utilizzano dati condivisi del Consorzio Universitario Piceno.

Art. 5 UTILIZZO DELLE STAZIONI DI LAVORO

Il personal computer affidato all'utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

Il personal computer dato in affidamento all'utente permette l'accesso alla rete solo attraverso specifiche credenziali di autenticazione come meglio descritto al successivo paragrafo (Rif. paragrafo 7.1 – Credenziali di accesso) del presente Regolamento.

Si rende noto che il Titolare del Trattamento (che si avvale dell'Amministratore di sistema) è autorizzato a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware etc.).

Art. 5.1 Utilizzo del personal computer

I personal computer assegnati a ciascun utente vengono adeguatamente configurati prima della consegna. Tale configurazione viene effettuata per ottimizzare e standardizzare le caratteristiche di ciascuna stazione di lavoro.

A ciascun utente è quindi vietato effettuare le seguenti attività:

- modificare la configurazione del sistema operativo o degli applicativi software installati (ogni modifica deve essere preventivamente autorizzata dal Titolare del Trattamento);
- gestire attraverso gli strumenti informatici aziendali informazioni personali non di interesse aziendale;
- salvare file o informazioni di qualsiasi tipo sul disco locale C:/, poiché i dati potrebbero andare persi. Tutte le informazioni dovranno essere salvate esclusivamente sulle unità di memorizzazione condivise e rese disponibili in rete. Qualora il personale autorizzato abbia documenti salvati sui dischi fissi è necessario quindi che venga effettuato un salvataggio in rete dei medesimi documenti, tempestivamente;
- disattivare software preimpostati per la protezione da virus informatici o per altri specifici scopi e installare altro software non autorizzato;
- compromettere il funzionamento dei servizi di rete e delle apparecchiature che li costituiscono con virus o programmi diretti a danneggiare o interrompere il funzionamento del Sistema;
- scaricare software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzati dal Titolare del Trattamento;
- effettuare ogni genere di transazione finanziaria a fini personali;
- registrarsi a siti i cui contenuti non siano legati all'attività lavorativa;
- partecipare a forum o bacheche elettroniche, iscriversi o loggarsi in social network, utilizzare strumenti di chat o messaggistica (esclusi gli strumenti autorizzati), anche utilizzando pseudonimi (o nickname), a fini personali.

Art. 5.2 Divieto di installazione di apparecchi non autorizzati

L'installazione e l'utilizzo di apparecchi non autorizzati (in particolare apparecchi di comunicazione quali chiavette UMTS, schede di rete, etc.) su postazioni di lavoro collegati alla rete aziendale offre una porta d'accesso dall'esterno non solo al computer, ma a tutta la rete aziendale senza protezioni.

Tale circostanza, espone a rischio di accesso abusivo tutti gli apparati e gli elaboratori connessi in rete e rende vani gli investimenti tecnologici effettuati dall'organizzazione per garantire la sicurezza di tutti gli asset del sistema informativo (firewall, sistemi di intrusion detection, ecc.).

È quindi vietata l'installazione da parte degli utenti di apparecchi non autorizzati in elaboratori aziendali. Per l'installazione e/o l'utilizzo di apparecchi originariamente non implementati nell'elaboratore affidato all'utente, quest'ultimo potrà farne richiesta al Titolare del Trattamento al fine di ottenere specifica autorizzazione, sulla base delle vigenti procedure aziendali.

L'installazione dovrà essere curata dal personale tecnico autorizzato, in base alle vigenti procedure di sicurezza.

Art. 5.3 Divieto di installazione di programmi non autorizzati

L'elaboratore è consegnato all'utente con alcuni programmi preinstallati. Tali programmi permettono l'esecuzione delle operazioni di trattamento cui è preposto l'utente stesso. Solo tali programmi e/o quelli successivamente installati da personale tecnico autorizzato, previa verifica della licenza d'uso, sono autorizzati.

Qualora per l'espletamento delle proprie mansioni sia necessaria o utile l'utilizzo di programmi specifici, gli utenti dovranno fare richiesta al Titolare del Trattamento al fine di ottenere specifica autorizzazione, sulla base delle vigenti procedure aziendali.

L'installazione dovrà essere curata dal personale tecnico autorizzato, in base alle vigenti procedure di sicurezza. In ogni caso, è assolutamente vietata l'installazione di programmi sugli elaboratori da parte del personale autorizzato e ciò a prescindere dal tipo di licenza (shareware o freeware) che ne regolamenti l'utilizzo.

Resta inteso poi che i programmi installati sugli elaboratori dovranno essere utilizzati per svolgere le proprie mansioni lavorative e non per un utilizzo personale.

Art. 5.4 Sospensione della sessione di lavoro e protezione degli elaboratori

Gli utenti sono tenuti ad assicurare che, durante la loro assenza dal posto di lavoro, le apparecchiature a loro assegnate siano in condizioni di sicurezza attuando, ove applicabili, le seguenti precauzioni:

- non lasciare visualizzate informazioni aziendali riservate;
- bloccare il personal computer con il comando Ctrl-Alt-Canc e selezionare "blocca".

Art. 6 UTILIZZO DI ELABORATORI PORTATILI

In aggiunta a quanto detto precedentemente, nel caso di utilizzo di personal computer portatili, occorre rispettare una serie di accorgimenti aggiuntivi.

Se all'utente viene fornito di un PC portatile, questi dovrà averne la massima cura e dovrà adottare tutte le precauzioni per ridurre al minimo i rischi di scambio o furto. Il PC portatile non può essere lasciato incustodito in macchina o in luoghi pubblici (a titolo esemplificativo ma non esaustivo: ristoranti, bar e treni). Se il PC portatile viene rubato, dovrà essere tempestivamente informato il Titolare del Trattamento e fatta relativa denuncia all'Autorità competente.

Gli utenti assegnatari degli elaboratori non devono mai lasciare incustodito il PC portatile.

Art. 7 ACCESSO AI SERVIZI

Art. 7.1 Credenziali di accesso (User ID e Password)

L'accesso ai Servizi Informativi di rete e al PC è subordinato al possesso di un identificativo aziendale (User ID) da utilizzare associato ad una parola chiave personale (Password).

L'utilizzo combinato di User ID e Password è, quindi, condizione necessaria per accedere alla Rete per l'attivazione di una "sessione di lavoro" e per l'utilizzo dei Servizi.

L'attivazione dei Servizi di Rete è concessa su base personale ed esclusivamente per ragioni e finalità connesse alle attività lavorative del titolare della User ID: pertanto non è consentito cedere a terzi, neppure temporaneamente, la "sessione di lavoro" o le informazioni necessarie ad attivarne una (User ID + Password).

A tutti gli utenti è fatto divieto di:

- accedere abusivamente ai Servizi di Rete;
- diffondere o detenere abusivamente Password;
- violare la sicurezza di archivi e computer;
- lasciare incustodite sessioni attive;
- utilizzare sessioni di lavoro di altri utenti.

Art. 7.2 Password di prima attivazione e password personale

La password iniziale attribuita dal Titolare del Trattamento all'atto della prima abilitazione di un utente è una password "usa e getta". L'utente è tenuto a cambiarla con una password personale al primo collegamento.

La Password personale è nota esclusivamente all'assegnatario della User ID collegata, deve essere custodita con diligenza ed attenzione e non deve essere comunicata a terzi, neppure temporaneamente.

Art. 7.3 Custodia della password

Le password devono essere mantenute segrete.

Gli utenti non devono:

- comunicare a terzi la propria password;
- scrivere la password in luoghi facilmente accessibili, né vicino alla postazione di lavoro;

In caso di assenza dell'utente, il recupero di file, documenti o dati cui lo stesso utente ha accesso esclusivo tramite le proprie credenziali di autenticazione, deve avvenire senza comunicazioni di password tra colleghi. In tali casi, deve essere informato il Titolare del Trattamento che, previa comunicazione all'incaricato assente, recupera i file, documenti o dati, rendendoli disponibili per le esigenze lavorative di terzi incaricati ed informando l'utente titolare del file.

Art. 7.4 Scelta della password personale

Il più semplice metodo per l'accesso illecito a un sistema informatico consiste nell'indovinare la password dell'utente legittimo. In molti casi sono stati procurati seri danni al sistema informativo a causa di un accesso protetto da password "deboli". La scelta di password "forti" è quindi parte essenziale della sicurezza informatica.

Di seguito vengono riportate alcune regole, che rappresentano lo standard in materia. Sebbene riportino alcune ripetizioni rispetto a quanto già detto in precedenza, si è ritenuto opportuno segnalare nuovamente il principio al fine di sensibilizzare l'utenza dei servizi di rete.

Cosa fare

1) Cambiare la password ogni qual volta richiesto dal sistema. Il sistema è impostato in modo da obbligare l'utente a modificare la password almeno ogni sei mesi.
2) Usare password lunghe almeno otto caratteri con un misto di lettere, numeri e segni di interpunzione, ovvero – laddove i sistemi gestiscano solo password di lunghezza inferiore – utilizzare password della lunghezza massima consentita dal sistema stesso.
3) Utilizzare password distinte per sistemi con diverso grado di sensibilità.
4) Qualora l'incaricato abbia notizia o timore che la propria password abbia perso la propria riservatezza deve modificarla immediatamente, avvertendo il Titolare del Trattamento.

Cosa non fare

5) NON comunicare a nessuno la propria password: lo scopo principale per cui le password sono usate è assicurare che nessun altro possa utilizzare le risorse affidate all'incaricato o che terzi possano farlo a nome dell'incaricato stesso.
6) NON scrivere la password da nessuna parte che possa essere letta facilmente, soprattutto vicino al computer.
7) Quando si immette la password nei form di richiesta, evitare che altri possano vedere i tasti che si battono sulla tastiera.
8) NON usare il proprio nome o altri dati anagrafici o di identificazione.
9) NON usare come password parole che possano in qualche modo essere legate alla propria persona come, ad esempio, dati del coniuge o familiari, ecc.

Art. 8 PROTEZIONE DA VIRUS

La prevenzione dalle infezioni da virus è molto più facile e comporta un impiego di tempo molto minore della correzione degli effetti di un virus e, tra l'altro, permette di evitare conseguenze quali la perdita irreparabile di dati. Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi. Alcuni virus si limitano a riprodursi senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido.

Come si trasmettono i virus informatici

I virus si trasmettono:

- attraverso programmi provenienti da fonti non ufficiali;
- attraverso le macro dei programmi di automazione d'ufficio;
- attraverso mail o risorse Internet.

Quando il rischio è alto

Il rischio di infezione da virus informatici è più elevato:

- quando si installano programmi;
- quando si copiano dati da supporti esterni;
- quando si scaricano dati o programmi da Internet;
- quando si aprono allegati provenienti da mittenti sconosciuti e/o non sicuri.

Effetti dei virus

Gli effetti tipici dei virus posso essere rappresentati dal fatto che:

- effetti sonori e messaggi sconosciuti appaiono sul video;
- nei menù appaiono funzioni extra finora non disponibili;
- lo spazio disco residuo si riduce inspiegabilmente;
- alcuni documenti vengono cancellati o rinominati.

Come "l'infezione"

Di seguito vengono evidenziate alcune linee guida per la prevenzione da virus informatici.

- utilizzare soltanto programmi installati dal personale tecnico autorizzato: copie non ufficiali di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato. È vietato l'uso di programmi non autorizzati.
- non aprire mai messaggi di posta elettronica provenienti da mittenti sconosciuti o che recano frasi "inusuali" nell'oggetto. Prestare particolare attenzione anche ai messaggi provenienti da utenti conosciuti che contengono allegati non identificati. Alcune "E-mail virus" sono in grado di inviare infezioni utilizzando il nome dell'utente registrato sul programma di posta elettronica che è stato infettato. È quindi teoricamente possibile ricevere un virus anche da un mittente conosciuto;
- non eseguire lo scaricamento (download) di programmi o documenti da siti Web dei quali non si ha la certezza dell'ufficialità o da link contenuti nel corpo di mail sospette;
- non utilizzare supporti esterni dei quali non si ha la certezza della provenienza;
- comunicare al Titolare del Trattamento qualsiasi messaggio inviato dai sistemi antivirus presenti sul proprio computer;
- non disattivare e/o modificare il software antivirus installato sull'elaboratore. Il Titolare del Trattamento provvede a curare un sistema di aggiornamento automatico degli antivirus installati sulle macchine assegnate agli utenti e ad effettuare verifiche, almeno, semestrali in merito. Qualora un utente si accorgesse del mancato funzionamento od aggiornamento del software antivirus installato sul proprio elaboratore è pregato di darne immediata comunicazione al Titolare del Trattamento.

Art. 9 POLITICA LOCALE DI BACK-UP

Come regola generale, gli utenti devono salvare i propri documenti nella rispettiva directory di rete, nessun documento aziendale dovrà mai essere salvato sul disco fisso del proprio elaboratore.

Qualora gli utenti abbiano documenti salvati sui dischi fissi è necessario un tempestivo salvataggio in rete dei medesimi (i dati custoditi in rete, infatti, vengono quotidianamente sottoposti a procedure di backup). In ogni caso, si ricorda che i files contenenti dati particolari (stato di salute, vita sessuale, opinioni politiche, religiose, sindacali, origini razziali o etniche, dati provenienti dal casellario giudiziale) devono essere salvati in rete e, qualora salvati su diversi supporti, protetti con password di accesso al documento, ovvero cifrati.

L'utente che, contravvenendo a quanto sopra, salvi dei dati sul proprio disco fisso sarà completamente responsabile della perdita di dati aziendali in caso di guasti al proprio elaboratore.

In caso di PC non collegati in rete, l'utente dovrà effettuare i Back-Up dei dati su disco esterno o chiavetta USB, almeno settimanalmente, da consegnare e mettere a disposizione del Titolare del Trattamento.

Art. 10 CONSERVAZIONE DEI SUPPORTI REMOVIBILI

I supporti removibili (Chiavette USB, ecc.) devono essere utilizzati e conservati in modo da evitare accessi non autorizzati e trattamenti non consentiti; ad esempio, quando non utilizzati, devono essere riposti in un contenitore o cassetto munito di serratura.

I supporti rimovibili contenenti dati particolari o giudiziari, se non più utilizzati, devono essere distrutti o resi inutilizzabili, in quest'ultimo caso provvedendo a cancellare i dati contenuti mediante formattazione del supporto stesso.

Nel caso in cui i supporti removibili debbano essere riutilizzati da altri collaboratori, non autorizzati al trattamento degli stessi dati (ad esempio, da personale non appartenente alla medesima area di lavoro), il riutilizzo dei supporti potrà avvenire esclusivamente qualora le informazioni precedentemente in essi contenute non siano intelligibili e tecnicamente in alcun modo ricostruibili.

Art. 11 UTILIZZO DI STAMPANTI E FOTOCOPIATRICI

Per quanto concerne l'utilizzo delle stampanti gli utenti devono assicurarsi di non lasciare incustoditi i documenti sulla stampante, ciò al fine di evitare che soggetti non autorizzati possano accedere ad informazioni personali, o di particolare riservatezza.

Per quanto concerne l'utilizzo delle fotocopiatrici gli utenti non devono allontanarsi dalla macchina durante la copiatura, per evitare che utenti non autorizzati entrino in contatto con i dati.

Art. 12 TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Gli utenti devono controllare e custodire per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali.

In particolare devono assicurare al termine dell'orario lavorativo l'archiviazione dei documenti nei cassetti della propria scrivania o nei rispettivi archivi. Tali operazioni dovranno rispettarsi ogni volta che l'utente stesso lo ritenga opportuno in considerazione della natura dei dati trattati e del periodo di tempo per il quale l'incaricato medesimo sarà lontano dalla propria postazione di lavoro.

L'accesso agli archivi contenenti dati particolari o giudiziari è permesso esclusivamente agli utenti autorizzati.

Nell'ipotesi in cui gli atti e i documenti contenenti dati personali particolari o giudiziari siano affidati agli incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti devono essere controllati e custoditi dagli stessi - fino alla restituzione - in maniera che ad essi non accedano persone prive di autorizzazione e siano restituiti al termine delle operazioni affidate.