Disciplinare per il trattamento dei dati e l'utilizzo degli strumenti informatici e telematici

Approvato con delibera di Giunta comunale n. 84 del 14 maggio 2019

ARTICOLO 1 – FINALITA'

1. Le responsabilità previste, in sede civile e penale, derivanti dalla diffusione delle tecnologie e dall'aumento di informazioni trattate con strumenti elettronici costantemente connessi ad Internet, impongono alla Pubbliche Amministrazione di garantire la continuità della sua attività e di assicurare l'integrità, la reperibilità, la riservatezza delle informazioni e dei dati trattati e la loro distruzione quando non più rilevanti per le attività istituzionali.
2. L'amministrazione deve operare in maniera tale da evitare che comportamenti consapevoli e/o inconsapevoli all'interno della stessa ed attacchi esterni possano diminuire l'efficienza e generare problemi alla sicurezza dei dati.

ARTICOLO 2 – GLOSSARIO

1. Per "**Utente**" deve intendersi ogni collaboratore abilitato alla connessione alla rete locale o in possesso di specifiche credenziali di autorizzazione per l'utilizzo delle risorse informatiche, a prescindere dal rapporto contrattuale intrattenuto: dipendenti, lavoratori somministrati, collaboratori a progetto, stagisti, consulenti ecc.
2. Per "**Risorsa**" si intende qualsiasi dato o strumento informatico e telematico di proprietà dell'Ente, utilizzato per rendere la prestazione lavorativa. A titolo esemplificativo ma non esaustivo sono risorse: i dati, i programmi, gli indirizzi e-mail inclusi i messaggi, i personal computer fissi e portatili, i tablet, i telefoni cellulari semplici o smartphone, i telepass, le carte di credito, i sistemi di geolocalizzazione e navigazione satellitare e i sistemi di antifurto satellitare installati su veicoli e la rete locale.

ARTICOLO 3 - PRINCIPI

1. Il Comune di Argenta, di seguito genericamente definito Ente, intende portare all'attenzione dei propri dipendenti e degli Utenti della rete locale, le linee di comportamento nel trattamento dei dati e per il corretto utilizzo degli strumenti messi a loro disposizione, quali ad esempio: personal computer fissi e portatili, posta elettronica e internet, inclusi i social network, definendone le modalità di utilizzo nell'ambito dell'attività lavorativa e dando la massima diffusione alla cultura sulla sicurezza informatica, intesa come consapevolezza e capacità dell'utilizzo delle risorse informatiche.
2. L'Ente, in qualità di titolare del trattamento di dati personali, si attiene, nella definizione del presente Disciplinare, agli obblighi fissati dal Regolamento Europeo sul trattamento dei dati personali (nel proseguo denominato "GDPR").
3. I trattamenti effettuati dall'Ente devono rispettare le garanzie poste in essere dal Legislatore in materia di protezione dei dati personali.

ARTICOLO 4 – REGOLE GENERALI DI COMPORTAMENTO

1. Il Comune di Argenta è titolare di qualsiasi diritto connesso ai sistemi e alle risorse informatiche, ai dati, ai contenuti di ogni genere, incluse le e-mail, elaborati creati o modificati, nell'ambito delle attività lavorative tramite l'opera dei suoi dipendenti e collaboratori.
2. L'utilizzo delle risorse, deve avvenire nell'ambito del più generale contesto di diligenza, fedeltà e correttezza che i dipendenti sottoscrivono con l'Ente. L'Utente dovrà adottare tutte le cautele necessarie per evitare le conseguenze dannose che un utilizzo non avveduto delle risorse produce.
3. L'Ente, consapevole delle potenzialità e dei rischi fornite dagli strumenti informatici e telematici, li mette a disposizione dei propri dipendenti e collaboratori esclusivamente per finalità di tipo lavorativo.
4. Non è quindi permesso utilizzare dette risorse per violare qualsiasi disposizione normativa o per finalità non connesse all'attività lavorativa.
5. Al riguardo si evidenzia che l'Ente adotterà ogni accorgimento tecnico necessario a tutelarsi da eventuali comportamenti non permessi, salvaguardano il rispetto della libertà e della dignità dei lavoratori.

6. Di seguito vengono descritte le linee di comportamento a cui gli Utenti devono attenersi, nell'esecuzione dei compiti che implicano utilizzo di risorse e il trattamento di dati di proprietà dell'Ente, nonché tutte le ulteriori misure ritenute necessarie per garantire il rispetto di quanto disposto dal Regolamento Europeo sulla Protezione dei Dati Personali n. 679/2016 (di seguito GDPR):
   a) Tutte le operazioni di trattamento devono essere effettuate in modo tale da garantire il rispetto delle misure di sicurezza e la massima riservatezza delle informazioni di cui si viene a conoscenza, considerando tutti i dati confidenziali e soggetti al segreto d'ufficio.
   b) Le singole fasi di lavoro e la condotta da osservare devono garantire che i dati non siano soggetti a rischi di smarrimento o distruzione o che vi possano accedere persone non autorizzate.
   c) Non devono essere eseguite operazioni di trattamento per fini non consentiti o non previsti dai compiti assegnati al diretto operatore.
   d) Devono essere svolte le sole operazioni necessarie per il raggiungimento dei fini per i quali i dati sono stati raccolti.
   e) Deve essere costantemente verificata l'esattezza dei dati trattati e la pertinenza rispetto alle finalità perseguite.
   f) Deve essere evitata la presenza di documenti duplicati al fine di evitare il disallineamento delle copie.
7. Quanto sopra descritto impone all'Utente di operare con la massima attenzione in tutte le fasi di trattamento, dalla esatta acquisizione dei dati, al loro aggiornamento, processo, conservazione o eventuale distruzione programmata.

ARTICOLO 5 – DISPOSIZIONI OPERATIVE

1. Uso del PC

Il personal computer (comprese le periferiche ad esso connesse) ed i relativi programmi e/o applicazioni affidati all'utente sono strumenti di lavoro; tali strumenti pertanto:
a) Vanno custoditi in modo appropriato.
b) Possono essere utilizzati solo per fini professionali e limitatamente alle mansioni assegnate; non ne è consentito l'uso a fini personali e tantomeno per scopi illeciti. Ogni utilizzo non inerente l'attività lavorativa è vietato perché può produrre disservizi, costi di manutenzione ed errata gestione dei dati. Eventuali minacce alla sicurezza debbono essere prontamente segnalati al SIA, così come il furto, il danneggiamento o lo smarrimento di dati o strumenti.
c) Il personal computer assegnato all'Utente permette l'accesso alla rete dell'Ente solo attraverso specifiche credenziali di autenticazione.
d) Non è consentito l'uso di programmi diversi da quelli ufficialmente installati ed autorizzati dal SIA, né viene consentito agli utenti la possibilità di installare autonomamente programmi provenienti dall'esterno, sussistendo grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti.
d) Per ogni modifica alla configurazione delle risorse informatiche assegnate, è necessario rivolgersi al personale del SIA.
e) Non è consentita la riproduzione o la duplicazione di programmi informatici ai sensi della Legge 21/05/2004 n. 128. L'inosservanza della presente disposizione espone a gravi responsabilità civili, amministrative e penali, nonché disciplinari, personali.
f) Non è consentito modificare le caratteristiche hardware e software del proprio PC.
g) Ogni Utente deve prestare la massima attenzione ai supporti USB forniti dall'Ente, avvertendo immediatamente il SIA, nel caso in cui siano rilevati virus.
h) Non è consentito collegare a PC dispositivi USB diversi da quelli forniti. Può essere valutata un'eccezione per i dispositivi USB di firma digitale di soggetti esterni, previo verifica su postazioni dedicate.
i) Si rimanda al comma 11, per quanto concerne i salvataggi dei file.
l) Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici. Analogamente il computer va spento in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. In ogni caso, lasciare un PC incustodito connesso alla rete con una sessione attiva può causarne l'uso improprio da parte di terzi senza che vi sia la possibilità di provarne in seguito l'altrui impiego.

2. Utilizzo di Pc Portatili

L'Utente è responsabile del PC portatile assegnatogli dall'Ente e lo deve custodire con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro. I PC portatili:

- utilizzati all'esterno dell'Ente, devono essere custoditi con diligenza, adottando tutti i provvedimenti necessari per evitare sottrazione, danni fisici o rischi informatici;
- non devono essere lasciati incustoditi e sul disco devono essere conservati solo i file strettamente necessari.

Nel caso di accesso alla rete aziendale tramite VPN (Virtual Private Network) o telecontrollo, deve essere utilizzato l'accesso in forma esclusivamente personale attraverso le credenziali di autenticazione fornite.
Al termine della sessione di collegamento, dovrà essere effettuata la disconnessione attraverso il software utilizzato.
I PC portatili, dovranno essere periodicamente collegati alla Rete interna al fine di consentire gli aggiornamenti antivirus.

3. Credenziali di autenticazione

Le credenziali di autenticazione per l'accesso al PC, per la connessione alla rete e/o per l'accesso ai diversi applicativi, vengono assegnate all'Utente dal SIA, in seguito alla sottoscrizione del contratto di assunzione o di collaborazione.
Le credenziali di autenticazione consistono in un codice per l'identificazione dell'Utente (user id), associato ad una parola chiave (password) riservata che dovrà essere custodita dall'Utente con la massima diligenza e non divulgata.
La password, che rappresenta la parte segreta delle credenziali, è conosciuta solo dall'Utente, è composta da almeno da 8 caratteri, deve essere formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, e non deve contenere riferimenti facilmente riconducibili all'Utente (nome, cognome, data di nascita ecc.).
L'Utente, ha l'obbligo di modificare la password dopo il primo utilizzo e la stessa va poi modificata periodicamente.
Per garantire la segretezza delle credenziali e la sicurezza durante le sessioni di trattamento dei dati, ogni Utente dovrà:
a) Evitare di condividere in qualsiasi modo la password;
b) Non lasciare accessibile l'elaboratore durante una sessione di lavoro;
c) Accertarsi che sia impostato uno screen saver dotato di password (con tempi di avvio brevi) che sia bloccato l'accesso all'elaboratore in caso di allontanamento prolungato;
d) Qualora il pc sia utilizzato da più incaricati, ricordare sempre di disconnettere la sessione di lavoro.
Le credenziali sono strettamente personali e non possono essere cedute a terzi. Il mantenimento della segretezza delle credenziali è ad esclusivo carico dell'Utente, il quale sarà il solo responsabile per qualsiasi attività posta in essere tramite l'utilizzo delle stesse.
In caso di smarrimento delle credenziali o di sospetta compromissione della sicurezza delle stesse, ne va fatta immediata segnalazione al SIA.
Non sono consentite credenziali generiche, non associate quindi ad un utente.

4. Antivirus

Il sistema informatico ed i pc collegati alla rete dell'Ente sono protetti da software antivirus a bordo e perimetrali aggiornati automaticamente.
E' vietato cancellare, riconfigurare o disattivare il software antivirus.
Ogni Utente è comunque tenuto a comportarsi in modo tale da ridurre il rischio di attacco al sistema informatico da parte di virus o attraverso qualsiasi altro software non sicuro.
L'Utente dovrà segnalare eventuali anomalie al SIA.

5. Utilizzo e Conservazione dei supporti rimovibili

Tutti i supporti magnetici rimovibili (CD e DVD riscrivibili, supporti USB, ecc. ma anche i documenti cartacei), contenenti dati personali, sensibili e/o informazioni riservate, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato, alterato, o distrutto o recuperato successivamente alla cancellazione. L'Utente è responsabile della custodia dei supporti e dei dati in essi contenuti.
Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati personali, ciascun Utente dovrà seguire la corretta procedura indicata dal SIA;
In ogni caso, i supporti contenenti dati personali devono essere adeguatamente custoditi dagli Utenti in armadi chiusi.
Non è consentito l'utilizzo di supporti rimovibili personali quali CD, chiavette USB, smartphone.

6. Utilizzo dei device (smartphone - tablet)

Gli utilizzi dei device forniti dall'Ente, non strettamente inerenti all'attività lavorativa, dovranno essere limitati a casi di urgente necessità ed improntati alla massima diligenza. Rimane inteso che è assolutamente vietato l'utilizzo dei device forniti dall'Ente, per la visione, il download ed il caricamento di contenuti contrari al buon costume o violenti. E' altresì vietato il download, la riproduzione e la condivisione di contenuti ottenuti illegalmente in violazione alla normativa sul diritto d'autore ed al codice penale.
Ogni utilizzo che possa in qualche modo contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza, è assolutamente vietato; qualora si riscontrassero addebiti o sanzioni sia sotto il profilo della responsabilità civile e penale, che di quella disciplinare, derivanti da un utilizzo improprio dei device, questi rimarranno a carico della persona che ha commesso l'illecito.
I device devono essere custoditi con cura evitando ogni possibile forma di danneggiamento.
L'Utente è responsabile dei device assegnati e deve custodirli con diligenza sia fuori che durante l'utilizzo nel luogo di lavoro.
I device utilizzati fuori dalla sede dell'Ente, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

7. Uso della rete aziendale

L'accesso alla rete dell'Ente avviene contestualmente all'inserimento delle credenziali di autenticazione per l'accesso al pc.
È assolutamente proibito entrare nella rete e negli applicativi con un codice d'identificazione Utente diverso da quello assegnato.
Le cartelle condivise presenti nei server dell'Ente sono aree di memorizzazione 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 vi può essere collocato.
Su queste unità vengono svolte regolari attività di amministrazione e back up da parte del SIA.
Si ricorda che tutti i dischi o altre unità di memorizzazione locali (es. disco C: interno al pc) non sono soggette a salvataggio da parte del personale incaricato del SIA.
La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo Utente.
E' vietato connettere in rete (via cavo o via radio) stazioni di lavoro o altri dispositivi hardware, diversi da quelli forniti dell'Ente. A titolo esemplificativo, ma non esaustivo, è vietato:
- Connettere alla rete aziendale personal computer personali o comunque non forniti dall'Ente;
- Connettere alla rete aziendale qualsiasi apparato di rete, (nas, switch, router, access point).

A tal scopo verranno attivate tutte le misure tecniche, atte ad impedire l'accesso alla rete da parte di qualunque dispositivo non autorizzato e censito dall'Amministratore di Sistema.

E' possibile connettere dispositivi forniti dall'Ente a reti e ad access point non forniti dall'Ente, purchè i dispositivi abbiano le necessarie protezioni come ad esempio:

1. che vengano osservate tutte le indicazioni di cui al preedente punto 2 "Utilizzo del PC portatile;
2. che siano dotati di antivirus aggiornato, e che vengano connessi frequentemente alla rete dell'Ente per i necessari aggiornamenti;
3. che l'utilizzo ordinario del dispositivo non avvenga con i privilegi di Amministratore per ridurre la superficie di attacco esposta a minacce esterne;

Il SIA potrà in qualunque momento e senza alcun preavviso rimuovere i dispositivi non autorizzati, dando seguito alle opportune azioni disciplinari nei confronti dei trasgressori.
E' vietato, se non appositamente predisposto dal SIA, ai sensi della vigente normativa, monitorare attraverso qualsiasi dispositivo hardware o software, ciò che transita in rete.
Per qualunque attività che preveda l'utilizzo della rete dati, è necessario informare e procedere in accordo con il SIA.

8. Uso della rete internet

La rete Internet è ormai divenuta uno strumento operativo di comunicazione imprescindibile, pertanto costituisce a tutti gli effetti uno strumento aziendale necessario allo svolgimento dell'attività lavorativa.
Un suo utilizzo non corretto, può rendere l'Ente vulnerabile sotto il profilo della sicurezza. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa. l'Utente deve usare internet in modo da non rivelare o diffondere informazioni di tipo confidenziale o di proprietà dell'Ente.

Non è consentito l'uso di sistemi di cloud storage, anche tramite applicazione web o di telecontrollo quali ad esempio DropBox o TeamViewer, tranne nei casi espressamente autorizzati.
Alla luce di ciò, l'Ente, anche per limitare il più possibile i controlli mirati, ha adottato alcune strumenti automatici di filtro ritenuti utili per proteggere i propri sistemi elettronici dall'eventuale utilizzo non accorto della navigazione su Internet da parte dei lavoratori.
In questo senso, a titolo puramente esemplificativo, l'Utente non potrà utilizzare internet per:
a) il download di software, nonché l'utilizzo di documenti, immagini, filmati e musica provenienti da siti non strettamente attinenti all'attività lavorativa;
b) l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dall'Ente e comunque nel rispetto delle normali procedure di acquisto;
c) ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
d) la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche come i social network e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dall'Ente;
e) l'accesso, tramite internet, a caselle webmail di posta elettronica personale.
f) è vietato l'uso di programmi elusivi, di file sharing o P2P e di streaming di contenuti non attinenti l'attività lavorativa anche se legali.
Al fine di evitare la navigazione in siti non pertinenti l'attività lavorativa, l'Ente rende nota l'adozione di un sistema di antivirus perimetrale e di filtro automatico che previene determinate operazioni quali l'upload o l'accesso a siti ad alta rischiosità inseriti in una black list.
I filtri sopra indicati limitano l'accesso a siti Internet che presentano i seguenti contenuti:
- illegali o non etici;
- materiale per adulti, pornografia;
- giochi, scommesse, intermediazione e trading, download software;
- social network, radio e tv internet;
- peer to peer;
- malware, spyware, hacking, bypass proxy, phishing.

Gli eventuali controlli, potranno avvenire 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 vengono conservati non oltre il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'Ente.

9. Uso della posta elettronica

La casella di posta elettronica assegnata all'Utente è uno strumento di lavoro. Gli utenti assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
Anche in considerazione del fatto che le caselle di posta elettronica e i loro contenuti sono di proprietà dell'Ente e che tali caselle, in particolari condizioni e con le necessarie autorizzazioni, possono essere aperte da altri addetti, è vietato utilizzare le caselle di posta elettronica istituzionali per motivi diversi da quelli strettamente legati all'attività lavorativa.
A titolo puramente esemplificativo, l'Utente non potrà utilizzare la posta elettronica per:
a) l'invio e/o il ricezione di allegati contenenti filmati o brani musicali (es. mp3) non legati all'attività lavorativa;
b) l'invio e/o la ricezione di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, acquisti online, forum o mailing-list se non legati all'attività lavorativa;
c) la partecipazione a catene telematiche (o di Sant'Antonio).
d) la ricezione di fatture per utenze personali.

Non si dovrà in alcun caso procedere all'apertura di allegati di messaggi non istituzionali.
La casella di posta deve essere mantenuta in ordine, cancellando allegati ingombranti, documenti inutili e dati sensibili non più necessari alla svolgimento delle attività lavorative.
Nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus contattare il SIA prima di procedere.
Nel caso di messaggi provenienti da mittenti conosciuti ma che contengono allegati sospetti (file con estensione .exe, .scr, .bat .reg ecc), o comunque in caso di dubbio, è necessario sincerarsi della veridicità della mail contattando il mittente stesso, è comunque utile contattare il SIA. E' necessario porre sempre la massima attenzione nell'aprire i file allegati di posta.Al fine di notificare agli interlocutori la natura esclusivamente istituzionale della casella di posta elettronica, i messaggi devono contenere un avvertimento standardizzato nel quale sia dichiarata la natura istituzionale e non personale dei messaggi stessi.
Pertanto, nei messaggi inviati tramite posta elettronica, verrà inserito il seguente testo:

"Avvertenza ai sensi del disciplinare Europeo sulla Protezione dei Dati Personali n. 679/2016.
Le informazioni contenute in questa comunicazione e gli eventuali documenti allegati, hanno carattere confidenziale, sono a uso esclusivo del destinatario e coperti dal vincolo della riservatezza. Nel caso questa comunicazione Vi sia pervenuta per errore, Vi informiamo che la sua diffusione e riproduzione ed il trattamento dei dati personali in essa contenuti, è contraria alla legge. Preghiamo di darci prontamente avviso e di cancellare quanto ricevuto."
Al fine di garantire la funzionalità del servizio di posta elettronica istituzionale e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) sarà compito dell'Utente impostare un messaggio di risposta automatica contenente le "coordinate" di posta elettronica di altro soggetto o altre modalità di contatto della struttura. Si ricorda che la risposta automatica deve essere attivata dall'Utente che potrà altresì impostare un inoltro automatico della posta in arrivo, ad un collega, delegato a gestire i messaggi ritenuti rilevanti per lo svolgimento dell'attività lavorativa.
In caso di assenza non programmata (ad es. per malattia) la procedura di risposta automatica - qualora non possa essere attivata dal lavoratore avvalendosi del servizio webmail entro due giorni - su richiesta del Responsabile della struttura di assegnazione del dipendente, potrà essere attivata a cura dell'Ente, avvalendosi del SIA, dandone comunicazione all'interessato appena possibile.
In caso di cessazione del rapporto di lavoro, la casella verrà definitivamente eliminata.
Tutto il contenuto verrà analizzato dal Dirigente del Settore di assegnazione del lavoratore cessato, che ne valuterà il destino.
Nessuna operazione di salvataggio dei messaggi eventualmente presenti, verrà effettuata a discrezione del personale del SIA dell'Ente.

10. Stampanti

Per quanto concerne l'utilizzo delle stampanti, gli utenti sono tenuti a:
- stampare documenti e atti solo se strettamente necessari per lo svolgimento delle proprie funzioni lavorative;
- prediligere le stampanti di rete in luogo di quelle locali al fine di ridurre l'utilizzo di materiali di consumo;
- le stampanti locali devono essere spente ogni sera prima di lasciare gli uffici.

Qualora l'Utente dovesse stampare documenti contenenti dati o informazioni riservate, dovrà avere cura di presidiare la stampante prelevando immediatamente le stampe. In caso di dimenticanza chiunque trovi tali documenti, se non è possibile identificarne il proprietario, è tenuto a distruggerli.
Qualunque configurazione delle stampanti di rete, sia al momento della prima installazione che successivamente, va fatta in accordo e tramite del SIA.

11. Gestione dati

L'Ente raccomanda di salvare frequentemente i documenti su cui si lavora ed in particolare, quando ci si allontani dalla postazione anche per breve tempo.
I dipendenti e collaboratori devono salvare i dati ed i documenti aziendali aventi importanza rilevante, in primo luogo nel software gestionale utilizzando gli strumenti messi a disposizione.
I documenti in lavorazione devono essere salvati su file server, nella cartelle appropriate. Ad ogni settore/servizio è attribuita una quota di spazio sul disco.
Costituisce comunque regola fondamentale la periodica pulizia di tutte le cartelle a cui si ha accesso sul file server, con cancellazione dei file obsoleti o che non hanno alcuna finalità e/o utilità per l'Ente.
Particolare attenzione deve essere prestata alla duplicazione dei dati. E' infatti assolutamente da evitare un'archiviazione ridondante.
Tutto ciò che viene memorizzato su file server è sottoposto a backup quotidiano, con una profondità di 7 giorni.
Resta comunque possibile memorizzare dati e documenti sul proprio PC, con la consapevolezza che in caso di guasto al disco, tutto potrà essere irrimediabilmente perduto.

12. Utilizzo di siti esterni per la conversione o verifica di file

L'utilizzo di programmi esterni per la conversione di documenti deve essere fatta con molta attenzione e con cognizione di causa.
A titolo esemplificativo ma non esaustivo l'utilizzo di siti che fanno una verifica antivirus o quelli concatenano pdf:
tale operazioni implica l'invio (upload) di documenti all'esterno con potenziale rivelazione di segreti d'ufficio, in caso di dubbi è sempre preferibile contrattare il SIA.

ARTICOLO 6 – MISURE A GARANZIA DELLA SICUREZZA DEL SISTEMA INFORMATICO

1. L'Ente ha l'obbligo di salvaguardare la funzionalità ed il corretto impiego degli strumenti informatici da parte dei lavoratori, pertanto, si riserva il diritto di effettuare controlli per verificare il rispetto del presente Disciplinare.
2. Le Risorse Informatiche sono di proprietà dell'Ente di appartenenza in quanto mezzo di lavoro. E' pertanto fatto divieto di utilizzo delle Risorse Informatiche e dell'accesso alla rete internet per fini ed interessi non strettamente coincidenti con quelli dell'Ente stesso. Con riferimento a tali controlli, il presente disciplinare costituisce preventiva e completa informazione nei confronti dei dipendenti e collaboratori.
3. Le verifiche sugli strumenti informatici saranno eseguite dall'Ente nel pieno rispetto dei diritti e delle libertà fondamentali degli utenti e del presente disciplinare, secondo i principi di pertinenza e non eccedenza.
4. L'Ente, pertanto, si riserva il diritto di controllare, in maniera occasionale e discontinua il corretto utilizzo degli strumenti di lavoro, implementando, però, ogni misura tecnologica volta a minimizzare l'uso di dati identificativi dei lavoratori, nei modi e nei limiti esplicitati di seguito e nel successivo paragrafo denominato "Graduazione dei controlli".
5. In nessun caso tali controlli verranno impiegati per un monitoraggio dell'efficienza dell'attività lavorativa del singolo individuo come prescritto dall'art. 4 Statuto dei lavoratori.
6. In prima istanza verranno abilitati strumenti atti ad impedire utilizzi impropri. I controlli si svolgeranno in forma graduata:
   a) in via preliminare l'Ente provvederà ad eseguire dei controlli su dati aggregati, riferiti all'intera struttura ovvero a sue aree e dunque un controllo anonimo che può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con invito ad attenersi scrupolosamente ai compiti assegnati ad alle istruzioni impartite;
   b) in assenza di successive anomalie non si effettueranno controlli su base individuale.
   In tali casi, il controllo si concluderà con un avviso ai dipendenti interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.
7. Nel caso vengano rilevate continue anomalie si procederà a controlli su base individuale o per postazione di lavoro (indicando le ragioni legittime, specifiche e non generiche, per cui i controlli saranno effettuati, inoltrando preventivi avvisi collettivi o individuali).

ARTICOLO 7 – MONITORAGGIO E CONTROLLO

1. L'accesso ai dati trattati dagli Utenti mediante utilizzo degli strumenti informatici messi a loro disposizione dall'Ente, avviene, da parte dell'Ente medesimo, per il tramite del S.I.A., conformemente alla normativa contenuta nel GDPR, prediligendo strumenti preventivi di sicurezza ed effettuando controlli esclusivamente in modi e tempi circoscritti ad eventi o proattivi in specifiche aree di rischio.
2. Gli strumenti utilizzati non possono e non intendono intercettare il contenuto dei file in transito, bensì si occupano solo di identificare la struttura dei dati in transito. Ad esempio, i filtri perimetrali della rete sono in grado di distinguere il traffico mail dal traffico p2p e bloccare quest'ultimo senza entrare in alcun modo nel contenuti trasportati.
3. Ogni utente è tutelato dai diritti sanciti dalla normativa sul trattamento dei dati personali. Egli può, in qualunque momento, richiedere delucidazioni, rivolgendo una specifica richiesta scritta al Titolare del trattamento.
4. L'Ente tiene in considerazione la difficoltà di tracciare una netta linea di confine tra l'attività lavorativa e la sfera personale e vita privata del lavoratore.
5. L'Amministratore di Sistema o i suoi delegati possono accedere ai dati trattati dall'Utente. Tali accessi sono registrati automaticamente su un registro informatico immodificabile e sono effettuati esclusivamente per motivi di sicurezza e protezione del sistema informatico (ad es., contrasto virus, malware, intrusioni telematiche, fenomeni quali spamming, phishing, spyware, etc.), ovvero per motivi tecnici e/o manutentivi e/o di regolare svolgimento dell'attività lavorativa (ad esempio, aggiornamento o sostituzione di programmi, manutenzione hardware).
6. A titolo esemplificativo, ma non esaustivo, il personale del SIA può accedere al PC di un Utente non presente, per l'installazione di un software, dandone comunicazione all'interessato, informandolo in merito alle attività svolte.

7. Il personale del SIA, in caso di assenza improvvisa o prolungata dell'Utente, può, per improrogabili necessità di sicurezza o di continuità di servizio accedere alla postazione dell'Utente, per le necessità operative. Di tale accesso dovrà comunque essere data tempestiva comunicazione all'Utente.
8. L'Amministratore di Sistema può procedere attraverso a specifici strumenti come ad esempio Qradar controlli anonimi, finalizzati a garantire l'operatività e la sicurezza del sistema o mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. Si intende per file di log la registrazione sequenziale e cronologica delle operazioni effettuate da un sistema informatico in formato testuale.
   Tale controllo viene effettuato in particolare sugli accessi effettuati dall'Amministratore di sistema. L'eventuale controllo sui file di log da parte dell'Amministratore di Sistema non è comunque continuativo ed è limitato ad alcune informazioni, ad esempio:
   a) Posta elettronica: l'indirizzo del mittente e del destinatario, la data e l'ora dell'invio e della ricezione e l'oggetto.
   b) Navigazione Internet: il nome dell'Utente, indirizzo IP della postazione, la data e ora di navigazione, il sito visitato e il totale degli accessi effettuati.
9. I file di Log vengono conservati per il periodo strettamente necessario per il perseguimento delle finalità organizzative, produttive e di sicurezza dell'Ente. Il sistema di registrazione dei log è configurato per cancellare periodicamente ed automaticamente (attraverso procedure di sovrascrittura) i dati personali degli utenti relativi agli accessi internet e al traffico telematico, fatti salvi casi definiti da specifica normativa.
10. In ogni caso, l'Ente garantisce la non effettuazione di alcun trattamento mediante sistemi hardware e software specificatamente preordinati al controllo a distanza, quali, a titolo esemplificativo:
    a) lettura e registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori (log) al di là di quanto tecnicamente necessario per il funzionamento del servizio;
    b) riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
    c) lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo.

ARTICOLO 8 - VIOLAZIONI

1. E' fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente Disciplinare. Il mancato rispetto o la violazione delle norme del presente disciplinare, è perseguibile nei confronti del personale dipendente con i provvedimenti disciplinari previsti dalla normativa vigente e dai regolamenti interni, nonché con le azioni civili e penali previste dalla normativa di riferimento.
2. L'amministratore di sistema e il personale del SIA, qualora ne vengano a conoscenza di violazioni alle norme suddette, sono obbligati a segnalarlo al Responsabile della struttura di assegnazione del dipendente o al Segretario comunale, in caso di dirigenti, in modo da dar seguito ai necessari accertamenti disciplinari.

ARTICOLO 9 – GESTIONE CREDENZIALI DI LIVELLO AMMINISTRATIVO.

1. Le credenziali di amministratore di tutti i server in gestione al Comune di Argenta sono segrete e vengono utilizzate solo ed esclusivamente in caso di emergenza. Pertanto sono note solo all'Amministratore di Sistema e al personale da esso autorizzato.
2. Il personale del SIA, sempre su autorizzazione dell'Amministratore di Sistema, è dotato di credenziali personali di livello amministrativo, relativamente alle proprie competenze. A titolo esemplificativo, ma non esaustivo, tutti gli accessi ai server sono effettuati con il proprio nome e quindi tracciati secondo il principio dell'accountability richiesto dal GDPR.
3. Nei casi in cui servissero credenziali amministrative generiche con password non rinnovata periodicamente, queste saranno gestite dal SIA.
4. Le credenziali di Amministratore di tutti i gestionali del Comune possono essere gestite dal SIA con le stesse modalità, solo tramite conferimento da parte del Comune stesso. In via esemplificativa le credenziali di amministratore del sistema di gestione del protocollo, dietro autorizzazione, possono essere detenute dal SIA per situazioni di emergenza. Tali credenziali, se gestite dal SIA, sono mantenute segrete e non vengono comunicate ad alcun

dipendente o collaboratore. Inoltre, sempre a seguito di autorizzazione, potranno essere create delle credenziali amministrative per il personale del SIA.

5. Nessun dipendente o collaboratore deve poter accedere a qualunque gestionale con credenziali amministrative generiche (del tipo admin e password) in quanto si perderebbe ogni forma di tracciabilità. Al contrario possono essere individuati ufficialmente utenti che potranno avere privilegi amministrativi.

ARTICOLO 10 - ASSISTENZA REMOTA DA PARTE DI DITTE ESTERNE

1. Il collegamento telematico di ditte esterne per qualunque tipo di assistenza deve essere preventivamente autorizzato dal SIA dell'Unione dei Comuni Valli e Delizie, tramite compilazione da parte della ditta di apposita modulistica. L'elenco delle ditte autorizzate sarà disponibile sulla pagina intranet.

ARTICOLO 11 - INFORMAZIONE

1. Al fine di informare i propri dipendenti dell'impatto del presente Disciplinare lo stesso sarà:

a) consegnato a ciascun dipendente ed a ciascun collaboratore ad inizio attività;
b) pubblicato sulla pagina intranet dell'Ente.