COMUNE DI ARESE

Regolamento per l'utilizzo degli strumenti informatici e telematici del Comune di Arese

Sommario

1. Premessa

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete tramite i personal computer, espone le organizzazioni a rischi di un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza e all'immagine.

L'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio di diligenza e correttezza, atteggiamenti questi destinati a sorreggere ogni atto o comportamento posto in essere nell'ambito del rapporto di lavoro.

Le attrezzature informatiche, i relativi programmi e/o applicazioni, i dati e documenti affidati in uso agli utenti sono strumenti di lavoro, di cui l'organizzazione può disporre indiscriminatamente, essendo titolare di qualsiasi diritto ad essi correlato. Tutto quanto messo a disposizione, ricevuto, rilasciato e comunque memorizzato per attività lavorative è e rimane di proprietà dell'organizzazione stessa.

Quanto indicato nel presente disciplinare rappresenta le istruzioni operative che permettono di effettuare una gestione dei sistemi a garanzia della sicurezza delle informazioni in conformità a quanto richiesto dal Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (da ora in poi GDPR).

La gestione delle risorse informatiche del Comune di Arese è in capo all'Ufficio Servizi partecipate e Servizi Informatici (d'ora in poi Ufficio Servizi Informatici o Servizi Informatici), che fa parte dell'Area Finanziaria e programmazione.

2. Scopo e campo di applicazione

Alla luce di quanto premesso, il Comune di Arese adotta il presente disciplinare interno al fine di

- evitare comportamenti inconsapevoli che possano innescare problemi o minacce alla sicurezza nel trattamento dei dati;
- informare i soggetti che trattano dati con le risorse informatiche di quali sono le misure di tipo organizzativo e tecnologico adottate all'interno dell'organizzazione per la sicurezza dei dati;
- illustrare quali sono le modalità di utilizzo consapevole e diligente delle risorse messe a disposizione;
- comunicare agli utenti le finalità e le modalità dei controlli che l'organizzazione potrebbe effettuare sulle risorse messe a disposizione;
- fornire agli utenti una serie di indicazioni operative sulle corrette modalità di trattamento dei dati personali, delle informazioni e degli strumenti che permettono di gestirli.

Le prescrizioni contenute nel presente documento si applicano a tutto l'insieme delle risorse informative, elettroniche, di comunicazione, di archiviazione, audiovisive, cartacee e a qualsiasi altra tipologia di risorsa utilizzata per perseguire le finalità istituzionali, siano esse di proprietà dell'organizzazione che di soggetti che operano in nome e per conto di esso.

3. Definizioni

ORGANIZZAZIONE: è la persona giuridica che adotta il presente documento, al fine di disciplinare l'utilizzo delle risorse informative, elettroniche, di comunicazione, di archiviazione, audiovisive, cartacee all'interno del proprio perimetro organizzativo e operativo di competenza.

SISTEMI INFORMATIVI: è l'abbreviazione della struttura preposta alla gestione, alla configurazione, al coordinamento e al rilascio delle risorse informatiche dell'organizzazione, a cui fanno riferimento gli Amministratori di Sistema competenti per tale contesto. Quando tale struttura è esterna all'organizzazione, essa svolge le proprie attività in nome e per conto di essa, agendo in qualità di responsabile del trattamento dei dati ai sensi dell'art. 28 GDPR.

AMMINISTRATORI DI SISTEMA: sono le figure, designate dal titolare o dai responsabili, che provvedono operativamente alla gestione e manutenzione del sistema informatico sulla base delle misure organizzative fissate dal responsabile dei servizi informativi, in linea con quanto indicato dal Garante della Privacy nel suo provvedimento del 27 Novembre 2008 e aggiornamenti successivi. Il provvedimento prevede la possibilità di nominare Amministratori di Sistema sia interni che esterni all'organizzazione: per le finalità del seguente documento si intendono gli Amministratori di Sistema preposti alla gestione delle risorse informatiche del titolare, siano essi interni o esterni.

UTENTI: sono i soggetti destinatari del presente disciplinare, a cui sono assegnate le risorse informatiche del titolare. Possono essere dipendenti, collaboratori o altri soggetti a cui le risorse sono assegnate per lo svolgimento di attività correlate alle finalità perseguite dal titolare.

DATO PERSONALE: qualsiasi informazione che possa ricondurre, in forma diretta o indiretta, ad una persona fisica identificata o identificabile. Se non diversamente espresso, il dato personale è sempre quello trattato dagli utenti esclusivamente per attività correlate alle proprie funzioni all'interno dell'organizzazione di riferimento.

DATO PRIVATO: qualsiasi informazione afferente ad utenti, non correlata alle funzioni da essi svolte nell'organizzazione di riferimento; tale contesto di riferimento non è pertinente o strumentale alle attività istituzionali del titolare.

DATO PROFESSIONALE: qualsiasi informazione trattata dagli utenti nello svolgimento delle proprie attività e funzioni esercitate nell'organizzazione del titolare.

TRACCIAMENTO: memorizzazione di eventi e operazioni effettuata automaticamente da un qualsivoglia dispositivo informatico, per finalità manutentive e di funzionamento dello stesso.

RILEVAZIONE: complesso di operazioni di raccolta, analisi, verifica, conservazione dei tracciamenti effettuati dai dispositivi e di qualsiasi altra forma di intervento di carattere professionale riferibile al funzionamento e all'utilizzo delle risorse informatiche, svolto a fronte di comprovate necessità definite nei capitoli seguenti del presente disciplinare.

DISPOSITIVO: qualsiasi strumento di elaborazione elettronica utilizzato per lo svolgimento delle attività che fanno capo all'organizzazione, il cui utilizzo rientra nel perimetro di competenza del presente disciplinare. Rientrano in tale definizione, a titolo esemplificativo e non esaustivo, desktop computer, notebook, tablet, ecc.

SUPPORTO DI ARCHIVIAZIONE: qualsiasi supporto elettronico destinato all'archiviazione e la custodia dei dati, come ad esempio chiavette USB, hard disk esterni, CD e DVD, ecc.

RGPD: viene così definito nel presente documento il Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

4. Obbligo di rispetto del presente disciplinare

Il rispetto del presente disciplinare è un obbligo per tutti coloro che utilizzano le risorse dell'organizzazione, in quanto rappresenta una garanzia di corretta gestione della sicurezza dei sistemi e dei dati personali.

Il mancato rispetto di quanto descritto dal presente disciplinare rappresenta una mancanza che potrà avere conseguenze di natura disciplinare o contrattuale – oltre che di potenziale rilevanza amministrativa o penale - in rapporto alla gravità del comportamento e dei potenziali rischi per il sistema e per i dati personali.

5. Dati trattati attraverso le risorse informatiche concesse in dotazione

Come disposto dall'art. 1 comma 4 del Regolamento concernente modifiche al decreto del Presidente della Repubblica 16 aprile 2013, n. 62, recante: «Codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165», pubblicato nella Gazzetta Ufficiale n. 150 del 29.06.2023: " 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."

In riferimento al Regolamento sopra citato, si precisa che le attività di carattere personale potranno essere svolte dal dipendente limitatamente alla pausa pranzo e comunque al di fuori dell'orario lavorativo. In tal senso, faranno fede le timbrature registrate sul cartellino del dipendente in ingresso, in uscita e in pausa pranzo.

Non è in alcun modo consentito o derogato l'utilizzo della strumentazione informatica per far fronte ad incombenze personali nel corso dell'orario lavorativo.

6. Utilizzo delle Postazioni di lavoro

La postazione di lavoro affidata agli utenti è uno **strumento di lavoro**. Ogni utilizzo non pertinente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza per cui va assolutamente evitato l'utilizzo improprio dello stesso.

Non è consentito acquistare, acquisire o installare programmi provenienti dall'esterno salvo, preventiva autorizzazione del personale incaricato dei Servizi Informatici, il quale, in rispondenza alle politiche di sicurezza dell'organizzazione ed alla normativa vigente, verificheranno l'opportunità (in termini di sicurezza dei sistemi) dell'installazione, onde evitare il grave pericolo di introdurre vulnerabilità, virus, nonché di alterare la stabilità delle applicazioni dell'elaboratore.

Non è consentito l'uso di programmi diversi da quelli messi a disposizione e autorizzati dall'organizzazione, in quanto l'inosservanza di questa disposizione, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'organizzazione a gravi responsabilità civili e penali in caso di violazione della normativa sulla

tutela del diritto d'autore (Legge 633 del 22 aprile 1941 sulla tutela della proprietà intellettuale, D.Lgs. 518 del 29 dicembre 1992 sulla tutela giuridica del software e aggiornamenti successivi), che impone la presenza nel sistema di software provvisto di regolare licenza d'uso.

Eventuali richieste di necessità di ottenere i privilegi amministrativi da parte di uno specifico utente, anche legato ad una singola azione (es. motivi tecnici legati a funzioni specifiche dei software), devono essere appositamente richieste, avvallate ed autorizzate dal personale dei Servizi Informatici.

Le attrezzature vengono consegnate agli utenti con una configurazione standard, coerente con le misure organizzative e di sicurezza impostate dall'organizzazione: non è consentito modificare le caratteristiche impostate, salvo preventiva autorizzazione degli Amministratori di Sistema incaricati.

La postazione di lavoro deve essere spenta prima di lasciare la sede di lavoro o in caso di assenze prolungate dalla sede, salvo specifica disposizione dell'Amministratore di Sistema o per espresse e specifiche contingenze che rendano necessario, in via del tutto eccezionale, derogare a tale prescrizione (es. Smartworking con collegamento su postazione fissa della sede lavorativa). In ogni caso, poiché lasciare un sistema di elaborazione incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'uso indebito, l'utente che lascia incustodita la postazione accesa deve bloccarne l'uso tramite la combinazione dei tasti CTRL + ALT + CANC e successivo INVIO dopo la scelta dell'opzione che dispone il blocco del computer.

Il blocco dello schermo verrà in ogni caso attivato, con la richiesta di password per lo sblocco, automaticamente dopo massimo 5 minuti di non utilizzo.

Non è consentito l'utilizzo di giochi o altre applicazioni di tipo ludico anche se comprese nel sistema operativo installato.

Non sono permesse le seguenti attività:

- caricare, memorizzare, pubblicare, diffondere, distribuire, tramite risorse dell'organizzazione documenti, informazioni, immagini, filmati etc. in generale, ed in particolare:
    - a carattere violento, pornografico o contrario alla pubblica decenza, o suscettibile di mancare di rispetto agli esseri umani o alla loro dignità, con contenuto discriminatorio razziale ed etnico, contrario al buon costume, oltraggioso nei confronti dei minori, contrario all'ordine pubblico, diffamatorio o che contenga contenuti illeciti penalmente o civilmente riconducibili a categorie qui non espressamente indicate;
    - illeciti in base alla normativa sul diritto d'autore;
    - pregiudizievoli per le risorse dell'organizzazione e per l'integrità e la conservazione dei dati dell'organizzazione stessa;
    - pregiudizievoli per l'immagine e il buon nome dell'organizzazione anche all'esterno del ristretto contesto dell'organizzazione;
- accedere a server web trattanti materie o soggetti ricadenti nelle categorie sopra elencate;

- tenere comportamenti che possano indurre taluno ad effettuare invii di materiale rientrante nelle tipologie sopra elencate; laddove l'utente riceva - anche involontariamente - tali materiali, è tenuto a informare il personale dei Sistemi Informativi ed attenersi alle istruzioni impartite circa il trattamento di tali materiali;
- utilizzare le risorse dell'organizzazione con fini di molestia, minaccia o comunque violando le norme di legge in vigore;
- caricare, memorizzare, trasmettere o utilizzare programmi, software, procedure od altra utilità che siano protetti dalle leggi sulla proprietà intellettuale, a meno che l'organizzazione non ne detenga regolare licenza e/o autorizzazione del produttore;
- utilizzare strumentazioni, programmi, software, procedure, etc.in violazione delle leggi sulla proprietà intellettuale, delle regole di buona condotta applicabili e delle prescrizioni emanate dall'organizzazione;
- caricare o trasmettere, con volontà, archivi o programmi contenenti virus o dati alterati;
- manomettere sistemi o archivi in maniera tale da inficiare la riservatezza, la disponibilità e/o l'integrità dei dati;
- inviare messaggi in massa ("spam") o favorire il propagarsi di notizie riconducibili a ciò che abitualmente viene definito "catena di S. Antonio";
- utilizzare le risorse dell'organizzazione in modo da consentire a soggetti non abilitati l'accesso ai dati e ad alle informazioni riservate, se non nei casi espressamente previsti dalla legge e/o da regolamenti interni.

La postazione viene fornita provvista di sistemi antimalware: l'utente deve verificare l'effettivo aggiornamento di tali sistemi, provvedendo al riavvio o allo spegnimento almeno settimanale della macchina.

In caso di anomalie dell'hardware e del software affidatogli, l'utente deve immediatamente bloccarne l'operatività, fermare le eventuali elaborazioni in corso ed informare immediatamente l'Ufficio Servizi Informatici per le incombenze di competenza.

L'esecuzione automatica dei contenuti dinamici (es. macro) presenti nei file non previsti dall'Ufficio Servizi Informatici in fase di configurazione, deve essere mantenuta disattivata.

7. Utilizzo Notebook e altri dispositivi elaborativi portatili (tablet, smartphone)

Ai dispositivi portatili si applicano le regole di utilizzo previste per i personal computer connessi alla rete descritte nell'articolo precedente.

Gli utenti di dispositivi portatili si impegnano, dovunque dovessero trovarsi, a mettere in sicurezza la strumentazione utilizzata e i dati nella stessa contenuti.

Danni arrecati alle attrezzature o loro perdita dovuti ad incauta custodia saranno a carico dell'utente utilizzatore.

L'utente è responsabile delle attrezzature informatiche portatili assegnategli dall'organizzazione e deve custodirle con diligenza, sia durante gli spostamenti sia durante l'utilizzo presso i luoghi di lavoro.

Il dispositivo non deve essere lasciato incustodito in zone a libero accesso, al fine di ridurre il rischio di furti. In caso di trasferte, il dispositivo non deve essere lasciato in macchina, nemmeno per brevi periodi, in parcheggi pubblici o comunque in zone non custodite.

Qualora tali dispositivi dovessero essere smarriti o rubati, l'affidatario deve immediatamente segnalare l'evento all'Ufficio Servizi Informatici, al fine di approntare le necessarie misure di mitigazione del danno e inoltre denunciare prontamente l'accaduto alle Autorità Competenti (es. Carabinieri, Polizia di Stato, altre Forze dell'Ordine.).

Nei casi in cui i dispositivi portatili siano di utilizzo condiviso e vengano messi a disposizione per attività episodiche (es. trasferte, presentazioni, meeting, etc.), l'utente deve considerare che tali risorse saranno messe a disposizione di altri utenti in momenti successivi, pertanto deve tassativamente rimuovere qualsiasi contenuto elaborato su di essi i prima della riconsegna, al fine di evitare incontrollate diffusioni di dati.

È in ogni caso tassativo rimuovere eventuali dati personali prima della riconsegna dei dispositivi.

8. Accesso remoto alle risorse informatiche dell'organizzazione

In caso sia necessario consentire ad un utente l'accesso remoto alle risorse informative, previa concessione del permesso da parte degli Uffici di competenza (es. per Smartworking), questo deve essere preventivamente concordato con il personale dell'Ufficio Servizi Informatici, e in caso specifico di utilizzo per Smartworking, deve attenersi all'Allegato 1 previsto nell'accordo Individuale di Lavoro Agile sottoscritto con il Personale.

9. Utilizzo dei supporti removibili

I supporti di memorizzazione rimuovibili attraverso i quali sono trattati dati dell'organizzazione devono essere utilizzati solo per attività lavorative.

Tutti i supporti esterni (cassette, secure drive, cd, dvd, dischi esterni USB, chiavette USB, SD cards, ecc…) contenenti dati personali trattati in ambito professionale devono essere utilizzati con particolare cautela onde evitare che il loro contenuto possa essere trattato da soggetti non autorizzati o esposti a minacce di sicurezza quali virus o altre vulnerabilità.

I dati personali salvati su supporti rimuovibili devono essere protetti tramite adeguati sistemi di cifratura, a tutela di possibili furti o smarrimenti. A tal proposito, prima della consegna ed assegnazione al personale, i supporti vengono cifrati tramite l'apposito software di sicurezza e possono essere utilizzati solo in modalità di cifratura attiva; in caso di particolari necessità tecniche o in assenza di dati personali sul supporto, potranno essere gestiti dei casi di sblocco della cifratura, solamente previa richiesta scritta del Responsabile di Settore che ne detiene la responsabilità e successiva autorizzazione e configurazione da parte dell'Ufficio Servizi Informatici.

I supporti contenenti dati personali, ancor più se sensibili e/o giudiziari, devono essere conservati con la massima attenzione da parte del personale che li utilizza: ogni eventuale conseguenza derivante dall'utilizzo inadeguato di detti supporti comporta una diretta responsabilità da parte dell'utilizzatore.

L'utente è responsabile dei supporti assegnati dall'Ente e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Possono essere utilizzati anche supporti removibili privati, il cui utilizzo viene concesso previa autorizzazione da parte dell'Ufficio Servizi Informatici, il quale provvederà a controllarne lo stato generale e l'assenza di virus o altre tipolgie di minacce e vulnerabilità.
In generale, è sempre preferibile evitare l'utilizzo di supporti removibili, qualora fossero presenti sistemi alternativi forniti ed autorizzati dall'Ente, quali ad esempio, l'utilizzo di cartelle e risorse in "cloud" o altro (risorse di sistema interno).

Qualora un supporto removibile dovesse presentare anomalie, l'utente deve bloccare immediatamente l'utilizzo ed avvertire tempestivamente l'Ufficio Servizi Informatici.

Ai fini di garantire la sicurezza del sistema informatico, l'organizzazione mantiene disattivata l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.

10. Trasferimento dei supporti di memorizzazione all'esterno dell'organizzazione

I supporti informatici di memorizzazione contenenti dati personali o informazioni riservate non possono essere portati all'esterno delle sedi dell'Ente se non previa autorizzazione del Responsabile di Settore competente. In tal caso, il Responsabile competente valuterà se i dati contenuti nei detti supporti debbano essere sottoposti a crittografia che, in caso di valutazione positiva, sarà eseguita dal personale dell'Ufficio Servizi Informatici.

11. Dismissione di dispositivi o supporti

In caso di necessità di dismissione di un dispositivo o di un supporto di memorizzazione, lo stesso dovrà essere preso in carico dall'Ufficio Servizi Informatici che si occuperà di effettuarne la dismissione rendendo illeggibili i dati contenuti.

Nel caso di riutilizzo di un dispositivo, l'Ufficio Servizi Informatici effettuerà la cancellazione dei dati precedentemente presenti prima di metterlo a disposizione per il nuovo utilizzo.

12. Utilizzo della rete LAN e delle risorse condivise

Al fine di garantire la disponibilità dei dati e un'efficace gestione dei backup, gli utenti che operano con postazioni fisse collegate alla rete LAN dell'organizzazione devono salvare su cartelle di rete tutti i file di lavoro che devono essere conservati ed eliminare i file non indispensabili. Per i file da conservare, gli utenti devono evitare di salvarli sul disco locale della postazione di lavoro come anche dei portatili in dotazione - si specifica che le cartelle "desktop" e "documenti" si trovano entrambe sulla postazione in locale, pertanto, sono inadatte al salvataggio dei file poiché non sottoposte a procedure di backup.

Le cartelle/unità di rete sono aree di condivisione 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.

Sulle cartelle/unità di rete vengono svolte regolari attività di amministrazione e backup secondo le politiche di configurazione e salvataggio definite a livello organizzativo.

Le cartelle di rete dovranno essere create (o rinominate) con nomenclature brevi (al massimo 20 caratteri per cartella), onde evitare il consumo massimo di caratteri totali per un percorso di file.

Le credenziali di ingresso alla rete ed ai programmi sono personali: è assolutamente vietato entrare nella rete e nei programmi con credenziali assegnate ad altri utenti.

L'Amministratore di Sistema, nell'espletamento delle mansioni attribuitegli per l'esercizio delle proprie attività, può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere potenzialmente pericolosi per la sicurezza, sia sulle postazioni di lavoro sia sui server.

Per la trasmissione di file all'interno dell'organizzazione è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati, oppure è possibile utilizzare le cartelle di scambio create a tale scopo. Le cartelle devono essere tenute in ordine, eliminando i file non più necessari.

Gli utenti dovranno effettuare la stampa dei dati solo se strettamente necessaria e dovranno ritirarla prontamente dai vassoi delle stampanti nel caso di utilizzo di stampanti condivise.

13. Utilizzo di piattaforme in cloud di file sharing

È possibile utilizzare piattaforme di file sharing solo se facenti parte della dotazione dell'organizzazione o previo nulla osta dell'Ufficio Servizi Informatici.

14. Acquisizione software

Sulle postazioni è consentita l'installazione esclusivamente delle seguenti categorie di software:

- software commerciale dotato di licenza d'uso (es. pacchetti di Office Automation);
- software gestionale acquisito specificatamente dall'Ente per lo svolgimento delle proprie mansioni lavorative (es. applicativi in uso ai vari servizi);
- software gratuito (freeware) e shareware prelevato dai siti internet, solo se espressamente autorizzato dall'Ufficio Servizi Informatici.
- qualsiasi altro software si renda necessario per l'esercizio delle attività lavorative, provvisto di una licenza non in contrasto con la normativa sul diritto d'autore ed a seguito di autorizzazione da parte dell'Ufficio Servizi Informatici.

In entrambi i predetti casi, i software devono essere sempre preventivamente valutati, autorizzati ed integrati nei sistemi dell'Ente in collaborazione con l'Ufficio Servizi Informatici, al fine di garantire la sicurezza, la stabilità dei sistemi presenti e la compatibilità del software con gli stessi.

15. Dispositivi con impatto sui sistemi informatici

La messa in opera di qualsiasi dispositivo o strumento che interagisca con la rete e/o la strumentazione informatica dell'organizzazione o possa avere un impatto con essi, qualora non venga eseguita direttamente dall'Ufficio Servizi Informatici, deve essere concordata preventivamente con detto Ufficio sin dalle primissime fasi di progettazione, onde evitare malfunzionamenti, cadute prestazionali, conflitti con altri sistemi o altri problemi e minacce relativi alla sicurezza ed all'immagine dell'organizzazione stessa.

Qualora venga affidata all'esterno la gestione di dati dell'organizzazione per l'erogazione di servizi, l'Ufficio competente deve concordare preventivamente con l'Ufficio Sistemi Informatici le

modalità e i formati con cui questi dati devono essere scambiati, sia in ingresso che in uscita, e le condizioni di consegna dei dati al termine del rapporto di collaborazione.

16. Gestione delle password e degli accessi

L'utente deve utilizzare sempre una password ogni qualvolta sia richiesto, avendo cura che nessuno ne venga a conoscenza.

L'accesso agli applicativi e ai sistemi può a sua volta essere regolato da un'ulteriore password: le modalità di gestione e di scadenza di dette password sono specifiche per ogni ambiente. All'utente sarà fornito un profilo personale e verranno attivate procedure per garantire all'utente stesso la conoscenza esclusiva della propria password. Nel caso il sistema non lo consenta o sia necessario l'intervento dell'Amministratore di Sistema per garantire la disponibilità dei dati, verranno concordate procedure specifiche per la gestione degli accessi.

La combinazione di username e password ai fini dell'accesso al dominio e agli applicativi garantirà la riservatezza dei dati personali e delle informazioni dell'organizzazione.

Se le credenziali sono comunicate agli utenti tramite comunicazioni elettroniche, user-id e password non devono essere comunicate tramite lo stesso canale di comunicazione. Qualora i canali di comunicazione utilizzati siano entrambi consultabili tramite un dispositivo (es smartphone, notebook, tablet, ecc), tale dispositivo deve essere a sua volta protetto dall'accesso di soggetti terzi.

Le password del dominio e degli applicativi, salvo impossibilità dovute all'obsolescenza o limiti del software, devono essere modificate ogni 3 mesi; devono essere formate da almeno 3 delle seguenti caratteristiche:

- caratteri maiuscoli

- caratteri minuscoli

- cifre decimali

- caratteri non alfabetici (es !,$,#,..);

devono avere una lunghezza di almeno 10 caratteri e non devono contenere riferimenti agevolmente riconducibili all'operatore (es. 2 caratteri consecutivi nel nome o cognome o nome utente).

Nel caso in cui si sospetti che una password abbia perso la segretezza, l'utente provvederà ove possibile a modificarla personalmente oppure con il supporto di uno degli Amministratori di Sistema.

Non è consentito utilizzare il profilo personale di altri soggetti per accedere ai sistemi. Qualora l'utente venga a conoscenza delle password di un altro utente, è tenuto a darne immediata notizia all'utente stesso o all'Ufficio Servizi Informatici.

L'utente è tenuto ad assicurare la segretezza delle password utilizzate per attività lavorative, al fine di garantire la sicurezza dei dati e dei servizi utilizzati.

17. Attività di backup dei dati utente

Sono oggetto di attività di salvataggio centralizzato su ambiente Cloud:

- i file salvati sulle cartelle/unità di rete messe a disposizione dall'Ufficio Servizi Informatici;

- le banche dati di applicativi ed i relativi file di sistema in uso per funzioni istituzionali, secondo le politiche di sicurezza definite;
- il contenuto delle caselle di posta elettronica gestite all'interno della piattaforma utilizzata dall'organizzazione, secondo le politiche di backup definite a livello organizzativo;
- il contenuto delle cartelle di storage assegnato agli utenti, secondo le politiche di backup definite a livello organizzativo.

I dati che risiedono sulle postazioni di lavoro (es: desktop) non sono soggetti a operazioni di backup centralizzato.

18. Attività e strumenti di assistenza remota

Per finalità di carattere manutentivo sono utilizzati sui dispositivi in dotazione strumenti di assistenza remota che consentono agli Amministratori di Sistema e, più in generale, al personale dell'Ufficio Servizi Informatici, di connettersi alle postazioni degli utenti per fornire supporto in tempo reale e assistere gli utenti nella risoluzione di problematiche di carattere informatico.

Gli strumenti utilizzati manifestano esplicitamente la connessione alla postazione da parte dell'Amministratore: l'utente dovrà consentire tramite autorizzazione verbale o informatica l'intervento remoto.

Qualora sia necessario consentire l'accesso e/o il controllo remoto da parte di soggetti esterni all'organizzazione per attività di carattere professionale, questo può essere fatto solo previa verifica dell'identità del soggetto che si connette alla risorsa e dell'effettiva necessità. Le attività effettuate da remoto devono essere monitorate durante il loro svolgimento. Qualora debba essere effettuato in orari di assenza del personale dell'organizzazione, prima di rilasciare l'accesso alla risorsa è necessario prendere dovute precauzioni al fine di ridurre l'accesso remoto solamente ai contesti per i quali si è reso necessario, senza che sia possibile per l'operatore remoto accedere, anche accidentalmente, ad altre informazioni.

19. Posta elettronica

La casella di posta elettronica, assegnata dall'organizzazione all'utente, è uno strumento esclusivo di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

Le caselle di posta assegnate dall'organizzazione possono essere utilizzate solo per finalità correlate alle attività istituzionali, pertanto, si assume che le informazioni veicolate tramite tale strumento non siano di carattere privato.

Qualsiasi attività istituzionale realizzata tramite utilizzo di posta elettronica deve essere svolta con l'esclusivo utilizzo di caselle registrate sotto il dominio di posta dell'organizzazione o tramite caselle di posta elettronica certificata registrate dall' organizzazione stessa. L'eventuale utilizzo di caselle non registrate sotto il dominio dell'organizzazione è consentito solo previa autorizzazione del Responsabile di Settore competente e dei Servizi Informatici: gli utilizzatori devono garantire il presidio di tali caselle e limitarne l'utilizzo allo stretto necessario.

È fatto divieto di utilizzare le caselle di posta elettronica dell'organizzazione per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list salvo diversa ed esplicita autorizzazione da parte del Responsabile di Settore e dei Servizi Informatici per esigenze di lavoro.

È vietato l'invio di messaggi con allegati di dimensioni superiori a 20 megabyte al fine di evitare sovraccarichi del sistema con conseguenti disfunzioni e rallentamenti della comunicazione aziendale.

La casella di posta deve essere tenuta in ordine evitando contenuti inutili.

Per la trasmissione di file all'interno dell'organizzazione devono essere usate le cartelle di scambio create a tale scopo e, in via del tutto eccezionale, la posta elettronica.

È vietato inviare e-mail con allegati i cui formati sono ritenuti pericolosi (es. estensione .exe, .bat, etc.). Il personale dell'Ufficio Servizi Informatici potrà impostare, attraverso appositi sistemi, il blocco di invio o ricezione di tipologie di file ritenute pericolose o non attinenti all'attività istituzionale ai fini della protezione dei dati e dei sistemi informatici.

È vietato aderire a catene telematiche (o di S. Antonio) che richiedono la divulgazione e circolazione di messaggi di posta di carattere non lavorativo. Qualora si ricevessero messaggi di tale tipologia, si dovranno cancellare i messaggi ricevuti senza divulgarli in alcun modo. Non si dovranno in alcun caso aprire o attivare gli allegati di tali messaggi.

Qualora si ricevessero messaggi sospetti di richiesta di password o altre informazioni oppure di invito a svolgere operazioni sulla propria postazione di lavoro (es. apertura o cancellazione di file, installazione aggiornamenti, apertura di una pagina web che richieda l'inserimento di credenziali, ecc.) di cui non è certa la provenienza, l'utente è tenuto a verificarli e a segnalarli immediatamente al personale dell'Ufficio Servizi Informatici, prima di effettuare qualsiasi altra azione.

È vietato utilizzare client (software) di posta elettronica differenti da quelli installati e configurati dall'Ufficio Servizi Informatici, a meno che non sia stata preventivamente concordata una differente procedura con il proprio Settore di competenza e con l'Ufficio Servizi Informatici. L'apertura automatica dei messaggi di posta elettronica è disattivata.

Le caselle di posta elettronica in uso presso l'organizzazione sono di 2 tipologie:

caselle nominative, assegnate con la convenzione <*nome_cognome*>@comune.arese.mi.it. Tali caselle sono intestate personalmente agli utenti: nonostante le caselle siano intestate ad un individuo, sono da considerarsi esclusivamente uno strumento di lavoro e non corrispondenza privata; pertanto, l'utilizzo verso destinatari esterni dovrà essere corretto e coerente con le funzioni istituzionali.

caselle di posta assegnate ad un ufficio o ad una funzione sul dominio @comune.arese.mi.it. Tali caselle sono configurate per lo scambio di posta verso l'esterno e possono essere assegnate a più persone. La continuità nella gestione della corrispondenza e delle attività ad essa correlate dovrà essere assicurata dal Responsabile di competenza, o dai Sistemi Informativi, attraverso opportune scelte organizzative.

Gli Amministratori di Sistema, nell'espletamento delle loro funzioni, potranno accedere alle caselle di posta assegnate per finalità manutentive solo in presenza dell'assegnatario della casella o su sua esplicita autorizzazione o su richiesta del diretto superiore in caso di indisponibilità dell'assegnatario stesso.

Al termine del rapporto di collaborazione, sulle caselle di posta nominative verrà attivato un risponditore automatico che segnalerà la cessazione del rapporto e indicherà un indirizzo alternativo nel dominio dell'organizzazione da contattare in caso di necessità di carattere professionale. La casella non sarà oggetto di consultazione, salvo che sia espressamente richiesto per finalità di continuità di servizio dell'organizzazione: in tal caso l'accesso dovrà essere adeguatamente motivato ed espressamente autorizzato dal responsabile dell'utente e il trattamento effettuato dovrà essere documentato.

La casella di posta verrà chiusa definitivamente entro 6 mesi, per garantire che eventuali comunicazioni su rinnovi automatici di servizi associati alla casella vengano adeguatamente reindirizzati.

In caso di situazioni di contenzioso o di precontenzioso tra l'utente e l'organizzazione, il contenuto della casella potrà essere conservato per tutta la durata del correlato procedimento, fino alla conclusione di tutti i gradi di giudizio.

20. Navigazione Internet

È consentita la navigazione internet agli utenti per lo svolgimento delle proprie mansioni lavorative.

La connessione ad Internet è uno strumento messo a disposizione per lavoro e per finalità correlate all'attività dell'organizzazione e ne è pertanto vietato l'utilizzo per fini non legati all'attività istituzionale.

Ogni utilizzo non inerente all'attività istituzionale può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla stabilità e sicurezza dei sistemi informatici; l'Ufficio Servizi Informatici potrà attivare pertanto tutti gli strumenti ritenuti necessari o anche solo opportuni per bloccare l'accesso ai siti ritenuti palesemente non pertinenti con le attività istituzionali o pericolosi per la sicurezza dei sistemi e dei dati personali.

È fatto assoluto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato dai siti internet, se non espressamente autorizzato dal proprio Settore Competente e dall'Ufficio Servizi Informatici.

A fini statistici, di qualità del servizio e di sicurezza, l'occupazione di banda generata dal traffico internet e dallo scambio di posta elettronica è soggetta a periodiche verifiche e controlli da parte dell'organizzazione.

Qualora i sistemi di sicurezza segnalino delle potenziali criticità che possano minare l'integrità dei dati e la stabilità del sistema stesso, potrebbero essere effettuati dei controlli sulla navigazione internet effettuata tramite la rete dell'organizzazione. Tali controlli si opereranno secondo stadi successivi:

1) controlli generici sulle pagine visitate, senza che vengano tracciati gli utenti che le visitano;
2) controlli aggregati sulle pagine visitate con suddivisione del traffico effettuato per aree lavorative;
3) controlli specifici sulle pagine visitate, con tracciamento dell'indirizzo IP da cui si effettua la visita o dell'utente che la effettua.

I controlli aggregati e specifici verranno effettuati solo qualora i trattamenti generici non abbiano consentito di risolvere le criticità riscontrate e verranno comunque segnalati in forma preventiva agli utenti.

Tutti i dati di traffico internet sono comunque sottoposti a tracciamento da parte di sistemi automatici implementati presso l'organizzazione e custoditi per il tempo strettamente necessario ad effettuare il controllo e risolvere la problematica riscontrata. La consultazione e conservazione di tali dati, al di fuori dei casi indicati precedentemente, è consentita:

- all'organizzazione stessa per attività difensive ovvero per far valere o difendere un diritto in sede giudiziaria. Qualsiasi trattamento verrà svolto dall'organizzazione nel rispetto della libertà e della dignità del lavoratore, in osservanza ai principi di pertinenza e non eccedenza;
- alle forze dell'ordine per attività di carattere ispettivo consentite dalla normativa sulla protezione dei dati delle persone fisiche.

21. Crittografia

L'utilizzo di sistemi di crittografia sulle risorse tramite cui vengono trattati dati di carattere professionale deve essere concordato con il personale dell'Ufficio Servizi Informatici.

Ogni attività di trasferimento verso l'interno e l'esterno dell'organizzazione di dati crittografati (sia tramite la connessione internet che tramite supporti fisici) dovrà essere concordata con il personale dell'Ufficio Servizi Informatici.

L'organizzazione potrà effettuare verifiche sui sistemi e sulle attività di copia, scarico, trasmissione dati e custodia, per accertare l'eventuale presenza di dati crittografati non preventivamente concordati.

22. Sicurezza generale e perimetrale

All'interno dell'infrastruttura tecnologica è attivato un sistema di sicurezza perimetrale a difesa dei sistemi e dei dati, che traccia eventi che possono essere indizio di minacce informatiche. Il sistema è soggetto a procedure di aggiornamento automatico per quanto riguarda la lista e le caratteristiche delle minacce.

È gestito da soggetti debitamente designati dall'organizzazione, i quali effettuano attività di verifica delle segnalazioni attivate dal sistema stesso, con lo scopo di comprendere e prevenire eventuali minacce esterne.

Qualora il sistema attivato rilevi delle minacce a specifici indirizzi IP interni delle postazioni di lavoro, l'Ufficio Servizi Informatici dell'Ente verificherà le cause della minaccia rilevata insieme all'utente/utenti che abitualmente utilizza/utilizzano la postazione, con l'obiettivo di comprendere la natura dell'intrusione e prevenire eventuali danni.

Una volta individuate le cause dell'evento rilevato verranno adottati provvedimenti correttivi, con segnalazione al Titolare dei trattamenti di eventuali violazioni alle regole indicate nel presente disciplinare.

23. Dispositivi mobili lasciati in dotazione

Tablet e altri dispositivi mobili (es. smartphone) forniti in dotazione ad utenti dell'organizzazione costituiscono uno strumento finalizzato al perseguimento di attività istituzionali e di carattere professionale.

L'utente deve fare tutto ciò che è nelle sue facoltà per prevenire eventuali furti di dispositivi in dotazione, prestando massima cautela nella loro custodia.

Al fine di ridurre il rischio di accesso ai dati residenti sul tablet e altri dispositivi mobili da parte di soggetti non autorizzati, l'utente deve attivare sistemi di blocco schermo con protezione con password numerica o con segno grafico composto sullo schermo o tramite riconoscimento dell'impronta digitale (in quest'ultimo caso deve essere messa a disposizione una modalità alternativa di accesso, per consentirne l'utilizzo anche ad altri utenti autorizzati).

Deve inoltre essere attivato automaticamente il blocco dello schermo entro un massimo di 5 minuti di inattività.

Il titolare del tablet o smartphone o altro dispositivo mobile è responsabile dell'aggiornamento software, delle APP installate nel dispositivo.

A causa della sempre maggiore interazione tra i dispositivi mobili e i sistemi informatici, l'abuso di tali strumenti può costituire una potenziale fonte di minaccia ai sistemi dell'organizzazione. Pertanto, è vietato:

- navigare su siti ritenuti non in linea con le indicazioni specificate nei precedenti capitoli relativi alla navigazione Internet;
- installare applicazioni sui dispositivi mobili assegnati dall'organizzazione senza previo accordo con il Responsabile dell'Ufficio che ha in dotazione i dispositivi e sentito il parere del personale dell'Ufficio Servizi Informatici;
- installare sulle postazioni di lavoro, d'ufficio o personali (private), programmi di sincronizzazione/backup dei dati contenuti sui dispositivi mobili potenzialmente dannosi senza la preventiva autorizzazione del Responsabile dell'Ufficio che ha in dotazione i dispositivi e sentito il parere del personale dell'Ufficio Servizi Informatici.

In caso di disservizio o di problemi di funzionamento software, i Servizi Informatici e le altre strutture preposte alla manutenzione dei dispositivi potranno effettuare dei controlli sulla configurazione dei programmi installati sull'apparato concesso in uso con finalità di protezione del patrimonio informativo. I controlli verranno effettuati nel rispetto della libertà e della dignità dei lavoratori; il trattamento di eventuali dati personali verrà effettuato nel rispetto dei principi di pertinenza e non eccedenza.

Qualora da tali controlli sopra menzionati dovesse emergere un utilizzo inadeguato delle attrezzature (fra cui l'installazione di programmi potenzialmente dannosi), che contravvenga le prescrizioni impartite, tale circostanza verrà comunicata alle strutture competenti che valuteranno l'eventuale adozione di provvedimenti.

Al momento della restituzione dei dispositivi, il personale assegnatario dovrà cancellare eventuali contenuti personali (es. e-mail, contenuti multimediali, ecc.).

Allorché il dispositivo restituito contenga dati personali, questi verranno cancellati indiscriminatamente dal personale incaricato dall'organizzazione prima di un'eventuale assegnazione successiva.

Per dispositivi particolari utilizzati per specifiche finalità (es. bodycam, attrezzature fotografiche mobili, ecc.) si rimanda a specifica documentazione regolamentare prevista dall'organizzazione.

In caso di smarrimento o furto di un dispositivo, è necessario segnalare immediatamente la circostanza all'Ufficio di competenza ed all'Ufficio Sistemi Informativi, al fine di valutare eventuali azioni di mitigazione del danno.

Si raccomanda di rimuovere il prima possibile immagini, video e audio e altri contenuti multimediali acquisiti tramite i dispositivi per qualsiasi motivo, al fine di evitare il rischio di divulgazione di dati personali in caso di furto o di smarrimento degli apparati.

24. Controlli

Le risorse messe a disposizione degli utenti sono strumenti attraverso i quali vengono perseguiti gli obiettivi istituzionali, su cui l'organizzazione gode di diritti esclusivi di proprietà e utilizzo. Il Titolare ha diritto di ottenere una corretta prestazione lavorativa e di attuare misure di sicurezza idonee alla difesa del patrimonio informatico.

Sulle risorse messe a disposizione potrebbero essere effettuati dei controlli, con le seguenti finalità:

- difendere il patrimonio dell'organizzazione;
- far valere o difendere un diritto in sede giudiziaria;
- tutelare gli interessi dei soggetti terzi che l'organizzazione è tenuta a salvaguardare nel perseguimento delle proprie attività istituzionali.

A questi fini, è prevista la possibile attuazione dei seguenti controlli:

- verifica di files e programmi presenti sui dispositivi che possano contravvenire le indicazioni specificate nel presente disciplinare, con la finalità di prevenire eventuali reati;
- controllo dei sistemi di accesso internet e di sicurezza perimetrale in caso di minacce segnalate dai sistemi di sicurezza o di lentezza di banda, con il fine di garantire il buon funzionamento della rete dell'organizzazione. Il controllo potrà riguardare l'occupazione di banda, l'utilizzo di sistemi di file sharing o la verifica di minacce segnalate dai sistemi di sicurezza;
- controllo della navigazione internet al fine di prevenzione di possibili minacce che possano compromettere la sicurezza dei sistemi informativi dell'organizzazione. Il controllo verrà effettuato a seguito della rilevazione di eventi non conformi agli standard di buon funzionamento, e verrà effettuato con profondità graduale come specificato nel precedente capitolo dedicato alla navigazione internet;
- accesso alla casella di posta degli utenti in caso di loro assenza e di necessità di dovervi accedere per motivi di continuità dell'attività lavorativa dell'organizzazione. In caso di accesso alla casella di posta, verrà redatto un apposito rapporto di intervento in cui verranno specificate la azioni intraprese, che verrà consegnato all'utente al termine del periodo di assenza;

- analisi dei dispositivi mobili messi a disposizione per attività di tipo professionale, con finalità di controllo della spesa e protezione dei dati ivi presenti. Le modalità di controllo sono specificate nell'apposito capitolo relativo ai dispositivi mobili in dotazione e alla telefonia mobile;
- controllo dell'esito dei backup effettuati sui sistemi server dell'organizzazione, con la finalità di garantire l'eventuale ripristino di dati o documenti in caso di necessità. Le verifiche potrebbero riguardare il controllo dell'esito dei backup o il ripristino casuale di un dato durante le fasi di test di ripristino effettuate per esaminare il buon funzionamento del sistema;
- controllo della messa in sicurezza dei dati lavorativi residenti sui dispositivi dati in uso, con la finalità di garantire la riservatezza e la disponibilità dei dati dell'organizzazione. Tale controllo riguarderà la verifica della localizzazione dei dati in spazi logici protetti e di misure di backup.

I controlli trovano fondamento nel bilanciamento tra gli interessi del datore di lavoro alla tutela del patrimonio aziendale quello alla tutela della privacy del lavoratore. Per tale ragione verranno condotti nel rispetto dei principi di correttezza e diligenza e nel rispetto dei principi privacy di necessità e proporzionalità. (DPO)

to indicato nel presente disciplinare e/o rispetto alle misure di sicurezza definite, l'organizzazione si riserva di intraprendere provvedimenti disciplinari.

A seguito di eventi che abbiano comportato un danneggiamento del patrimonio di proprietà dell'organizzazione, qualora emergano degli elementi che possano fondatamente evidenziare degli atteggiamenti inadeguati potenziale causa dei danni rilevati, l'organizzazione ha diritto di attuare controlli difensivi occulti con la finalità tutelare le risorse in uso, se da essi fosse possibile riscontrare e sanzionare un comportamento idoneo improprio da parte degli utenti.

25. Sistemi di monitoraggio attivo dei dispositivi e del software

I dispositivi elettronici tracciano una serie di eventi di sistema per attività amministrative, manutentive e/o di sicurezza, che variano a seconda della tipologia dei dispositivi stessi.

Sono attivi specifici sistemi di monitoraggio di rete, server, personal computer, notebook etc… che permettono di ottenere informazioni sui sistemi e sul traffico generato dagli stessi al fine di monitorare il corretto funzionamento di tutto il sistema informatico, prevenire e correggere eventuali disfunzioni.

Tali sistemi effettuano il monitoraggio in maniera automatica e senza richiedere il consenso agli utenti delle postazioni monitorate.

Esempi di tali tipologie di monitoraggio sono:

- Rilevazione e inventario dispositivi hardware utilizzati
- Rilevazione e inventario dei software presenti sui dispositivi
- Analisi del software presente sui dispositivi non compreso nell'elenco dei software autorizzati

- Monitoraggio ed alert in caso di anomalie del traffico di rete interna e del funzionamento delle postazioni di lavoro
- Installazione automatica sulle postazioni di lavoro di applicazioni ed aggiornamenti
- Filtraggio dei messaggi di posta elettronica con sistemi antispam o similari
- Filtraggio dei messaggi di posta elettronica per blocco tipologie di file ritenute pericolose
- Analisi dei contenuti del traffico web per filtraggio tipologie di file ritenute pericolose
- Blocco di esecuzione di file ed applicativi ritenuti pericolosi attraverso il sistema di antivirus
- Raccolta log di sistemi operativi, applicativi, utility, sistemi di protezione
- Filtraggio e blocco siti web ritenuti non adeguati
- Filtraggio e segnalazione trasferimenti di files criptati non previsti
- Analisi ed identificazione delle vulnerabilità e dei sistemi
- Discovery di sistemi e attività che possano ledere la sicurezza delle risorse

I Sistemi Informativi potranno impostare attraverso sistemi hardware o software il blocco di invio o ricezione di un tipologie di file ritenute pericolose ai fini della protezione dei dati e dei sistemi informatici.

Per quanto riguarda i controlli che potrebbero essere svolti sulla navigazione internet degli utenti si rimanda al precedente capitolo dedicato al tema.

26. Osservanza del presente disciplinare

In caso si riscontrino delle criticità che possano ledere la sicurezza del sistema informativo, l'organizzazione potrà verificare che l'utilizzo delle risorse strumentali concesse in dotazione agli utenti sia conforme alle indicazioni riportate nel presente disciplinare.

Il mancato rispetto delle regole e delle misure di sicurezza elencate nel presente documento implica la responsabilità personale dell'utente.

27. Entrata in vigore

Il presente regolamento entrerà in vigore il 01.01.2024.