anci toscana

DISCIPLINARE INTERNO sull'USO di INTERNET, POSTA ELETTRONICA e ALTRI STRUMENTI INFORMATICI

ancitoscana.it

INDICE

INTRODUZIONE

Anci Toscana può mettere a disposizione del proprio personale e di eventuali collaboratori e consulenti i seguenti strumenti di lavoro, in funzione del loro ruolo e delle esigenze lavorative:

- strumenti di informatica individuale quali personal computer, laptop, smartphone e relativi accessori;
- apparati e servizi condivisi quali ad esempio posta elettronica, accesso alla rete, stampanti di rete, scanner file server, spazio cloud condiviso, ecc.
- programmi di produttività individuale e gestionali accessibili via web.

Tali risorse costituiscono un mezzo di lavoro e devono essere utilizzate, di norma, per il perseguimento di fini strettamente connessi agli incarichi lavorativi secondo criteri di correttezza e professionalità, coerentemente con il tipo di attività svolta e in linea con le disposizioni normative vigenti.

Il documento illustra le norme generali di utilizzo delle suddette risorse che il personale, i collaboratori e i consulenti devono rispettare al fine di mitigare i rischi che un uso improprio delle stesse può determinare alla sicurezza del patrimonio informativo e all'immagine dell'Associazione.

Nella definizione delle norme comportamentali da osservare si è tenuto conto di quanto previsto dalla normativa vigente in materia e, in particolare, dal Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" e s.m.i. e del Regolamento 679/2016.

CAMPO DI APPLICAZIONE

Le regole descritte nel presente documento devono essere rispettate da tutto il personale dipendente di Anci Toscana, dai collaboratori e dai consulenti per le parti a loro afferenti, indipendentemente dal tipo di incarico svolto e dalla sede dell'attività.
La gestione delle risorse informatiche compete ai Dirigenti ed alle Posizioni Organizzative, per la parte delegata, che si assumono l'onere di vigilare sul corretto utilizzo e sull'osservanza delle norme da parte del personale a loro assegnato.

NORMATIVA DI RIFERIMENTO

Il presente Disciplinare Interno è redatto in conformità alla normativa vigente, di seguito riportata per riferimento:

- Normativa in materia di diritto d'autore e di altri diritti connessi al suo esercizio introdotta con la Legge n.633/4, aggiornata con le modifiche apportate dalla L. 3 maggio 2019, n. 37 per la protezione delle opere dell'ingegno di carattere creativo qualunque ne sia il modo o la forma di espressione

- Normativa in materia di protezione del software introdotta con il D.Lgs. n.518/92 "Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratori"; tale provvedimento normativo ha infatti aggiunto l'art. 171-bis, avente ad oggetto la tutela di programmi per elaboratori, all'art.171 della Legge n° 633/1941. L'art. 171-bis, il cui testo è stato ultimamente modificato dalla L. n° 248/2000 "Nuove norme di tutela del diritto d'autore", prevede sanzioni penali a carico di coloro che duplicano, detengono, distribuiscono o vendono programmi per elaboratore oggetto di copyright; pertanto la norma pone il divieto assoluto di fare copie illegali di materiale protetto da leggi a tutela del diritto d'autore e di rendere tale materiale disponibile a terzi per effettuarne delle copie

- Legge 20 maggio 1970, n. 300 "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento" (Statuto dei Lavoratori) aggiornato, da ultimo, con le modifiche apportate dal D.Lgs. 24 settembre 2016, n. 185

- Costituzione della Repubblica Italiana, art. 15 sancisce che "La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge"

- Codice Penale art. 616 - Violazione, sottrazione e soppressione di corrispondenza

- Regolamento 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

- Codice della Privacy coordinato ed aggiornato con le modifiche apportate dalla L. 27 dicembre 2019, n. 160, dal D.L. 14 giugno 2019, n. 53, dal D.M. 15 marzo 2019 e dal Decreto di adeguamento al GDPR (Decreto Legislativo 10 agosto 2018, n. 101): garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali e della dignità dei soggetti a cui si riferiscono i dati, imponendo l'adozione di misure di sicurezza che riducano il rischio informatico e consentano un efficace controllo sull'utilizzo e la conservazione dei dati. Il decreto prevede un livello minimo di sicurezza per i dati personali definendo le misure fisiche, logiche e organizzative che devono essere adottate al fine di evitare possibili distruzioni, perdite, alterazioni di dati; garantire che l'accesso ai dati sia effettuato dalle sole persone incaricate al trattamento e quindi autorizzate; garantire che il trattamento avvenga per le finalità e nelle modalità consentite

- Circolare Agenzia per l'Italia Digitale 18 aprile 2017, n.2/2017 "Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)".

- Le misure di sicurezza sono applicate garantendo il rispetto della normativa vigente in materia.

- Art. 2014 e art 2015 del Codice Civile (Diligenza del prestatore di lavoro)

UTILIZZO DELLE POSTAZIONI DI LAVORO

Principi generali

In funzione del proprio ruolo e delle esigenze organizzative e lavorative, i soggetti che a vario titolo svolgono attività per Anci Toscana possono essere dotati di personal computer, laptop, smartphone, per l'attuazione delle attività stesse connesse agli incarichi lavorativi.

Ognuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione dall'Associazione.

Viene quindi posto l'obbligo, in carico ai responsabili dei diversi Settori, di vigilanza sui dipendenti assegnati al fine di verificare l'effettivo adempimento della prestazione lavorativa e il corretto utilizzo degli strumenti di lavoro. Ogni abuso in tal senso dovrà essere prontamente rilevato ed eventualmente sanzionato.

Per quanto attiene ai dispositivi privati (non di proprietà di Anci Toscana) connessi alla rete di Anci Toscana non si applica quanto previsto dal presente disciplinare riguardo alle postazioni di lavoro limitatamente al paragrafo "Utilizzo delle Postazioni di lavoro" sezione "Regole di utilizzo".
In caso di uso di dispositivi privati Anci Toscana si riserva comunque la facoltà di effettuare controlli di sicurezza al momento della connessione degli stessi dispositivi alla rete e di registrarne le informazioni nei report di sicurezza.
In caso di utilizzo di risorse informatiche private (tablet, smartphone, periferiche etc.), l'utente è tenuto a rispettare le misure minime di sicurezza descritte nell'allegato B del D.Lgs 196/2003 (INFO: https://www.camera.it/parlam/leggi/deleghe/03196dl3.htm#ALLEGATO%20B) *e ssmm;*

Regole di utilizzo

Le postazioni di lavoro, normalmente, sono connesse alla rete interna di Anci Toscana per consentire l'utilizzo dei servizi all'interno degli uffici. Questi riguardano l'accesso alla rete, l'uso delle stampanti e scanner, l'accesso al server e ai servizi in cloud.

Per una corretta gestione delle postazioni di lavoro è necessario osservare alcune regole:

- Le informazioni archiviate nella postazione devono essere inerenti la propria attività lavorativa
- Il salvataggio (backup) dei dati necessari all'attività lavorativa per le postazioni che non memorizzano i propri dati sul server centrale è di esclusiva responsabilità dell'utente
- La modifica dei componenti interni (aggiunta, rimozione, sostituzione) delle attrezzature informatiche non è consentita
- La modifica delle configurazioni software impostate sulla propria o altrui postazione di lavoro è consentita da parte dell'utente esclusivamente su autorizzazione della P.O. o del Dirigente di riferimento, fatto salvo per le operazione di aggiornamento di sicurezza dei sistemi operativi e dei software autorizzati (vedi lista), che devono essere effettuati autonomamente dal singolo utente al momento del suggerimento da parte del sistema operativo e/o dei software installati;
- L'attivazione o la modifica di password di sistema sono lasciate alla libera scelta dell'utente, sotto la propria responsabilità
- Non è consentita l'installazione di programmi applicativi diversi da quelli inseriti nella lista scaricabile al seguente link. La lista è costantemente aggiornata tenendo conto delle necessità operative manifestate dal Dirigente e dalle Posizioni organizzative. Qualora venissero riscontrati programmi non autorizzati sulle postazioni di lavoro, anche se legali, si procederà con la disinstallazione

- La riproduzione o la duplicazione di programmi può essere effettuata solo nel pieno rispetto della vigente normativa in materia di protezione della proprietà intellettuale

- Si sconsiglia l'uso di supporti di memorizzazione di incerta provenienza che potrebbero causare danni alla postazione di lavoro. L'utilizzo di memorie USB, data l'estrema facilità con cui possono prestarsi alla diffusione di virus e malware, è da effettuarsi con massima attenzione

- È proibito duplicare documenti contenenti dati sensibili su supporti removibili o su sistemi di rete non autorizzati dall'Associazione

- In caso di smarrimento o furto di dispositivi informatici, oltre a sporgere regolare denuncia all'autorità competente, informare tempestivamente la P.O. Risorse umane e organizzazione comunicando quali dati erano contenuti all'interno; al termine del lavoro deve essere correttamente chiusa la sessione e devono essere spenti computer, video ed accessori

- Costituisce buona prassi effettuare con cadenza periodica (almeno ogni sei mesi) la pulizia degli archivi presenti sulla propria postazione e nelle cartelle di rete di propria competenza, con cancellazione dei file inutili o obsoleti. Si deve porre particolare attenzione ad evitare un'archiviazione ridondante con duplicazione dei dati
- La tutela della gestione locale dei dati presenti sugli strumenti in dotazione è demandata all'utente finale che dovrà effettuare, con frequenza opportuna, salvataggi su cloud o supporti di rete
- Nel caso in cui esista la necessità di elaborare banche dati in locale, ad esempio su fogli di calcolo o database personali, è necessario adottare le misure di sicurezza idonee a garantire il rispetto della normativa in materia di tutela dei dati personali

L'utente è responsabile delle attrezzature che gli sono affidate in uso e pertanto deve provvedere a mantenerle in completa efficienza segnalando tempestivamente al Dirigente o alla propria P.O. di riferimento ogni eventuale problema tecnico

L'Associazione utilizza alcuni software (presenti nella lista autorizzata) che, per fornire assistenza, permettono di vedere in tempo reale le attività svolte dal lavoratore solo quando strettamente necessario dietro esplicita accettazione da parte dell'utente attraverso la comunicazione del codice univoco di accesso generato dal software.

CREDENZIALI E PASSWORD

Principi generali

Le credenziali (nome utente e password) vengono rilasciate al momento della creazione di un'utenza dopo che Il Dirigente o la P.O. di riferimento ha appurato la necessità di accedere o utilizzare un servizio.

Regole di utilizzo

Per una corretta gestione delle credenziali di autenticazione è necessario osservare le seguenti regole:

- Modificare alla prima connessione la password che si attribuiscono e comunicano

- Modificare la password almeno ogni sei mesi (password aging), nel caso di trattamento di dati sensibili e/o giudiziari, almeno ogni 90 giorni secondo le disposizioni contenute nell'allegato B del D.Lgs 196/2003 e ssmm; non utilizzare password simili a quelle precedentemente usate (password history); nel caso in cui si ritenga che la propria password sia stata compromessa, modificarla immediatamente

- Mantenere le password personali riservate, non divulgarle a terzi l'utente è responsabile penalmente e civilmente di abusi o incidenti di sicurezza nel caso in cui non custodisca adeguatamente le proprie credenziali personali

- Non trascrivere le password su supporti facilmente accessibili a terzi (ad es. foglietti, post-it etc.)

- Comunicare tempestivamente al Dirigente o alla P.O. di riferimento trasferimenti e cessazioni, in modo da consentire la disabilitazione dell'accesso ai servizi non strettamente necessari

Si fa presente però che in caso di prolungata assenza o impedimento dell'utente, che renda indispensabile ed indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, Il Dirigente o la P.O. del settore di assegnazione dell'utente, è autorizzato ad attivare la procedura per il reset della password dell'utente stesso.

NOTA: si allega per comodità degli utenti il documento del GPDP "Suggerimenti per creare e gestire password a prova di privacy"

USO DELLA POSTA ELETTRONICA e Spazio Cloud

Principi generali

Anci Toscana fornisce ai propri dipendenti, ed eventualmente ai propri collaboratori e consulenti, un account di posta elettronica, mettendo a disposizione indirizzi con estensione @ancitoscana.it e un relativo spazio di archiviazione cloud. Gli account possono essere individuali o afferenti a un servizio; questi ultimi vengono richiesti dal Dirigente o dalla P.O. di riferimento dello stesso e possono essere condivisi tra più lavoratori. Il servizio di posta elettronica è uno strumento di lavoro e deve essere di norma utilizzato per lo svolgimento di attività connesse agli incarichi lavorativi e/o istituzionali. Il database di posta è di esclusiva proprietà dell'Ente. Per motivi tecnici e di sicurezza, Il Dirigente o la P.O. del settore di assegnazione dell'utente è autorizzato ad attivare la procedura per accedere al suo contenuto nel rispetto della normativa vigente.

Regole di utilizzo

Per l'uso del servizio di posta elettronica, si richiede di osservare le seguenti norme comportamentali:

- L'uso della posta elettronica aziendale è consentito esclusivamente per motivi attinenti allo svolgimento delle mansioni assegnate; l'utente del servizio è consapevole che i contenuti della posta elettronica dell'Associazione non devono avere carattere privato o personale, ma devono riguardare esclusivamente questioni connesse all'attività lavorativa

- L'accesso alle caselle di posta avviene da remoto

- Il titolare di indirizzo di posta elettronica ha il dovere di controllare periodicamente la propria casella elettronica e lo spazio cloud relativo, verificare l'arrivo di nuovi messaggi, cancellare file e messaggi obsoleti o inutili, verificare lo spazio occupato, prestare attenzione ai messaggi di quota raggiunta, ripulire la casella ed ottimizzarne il più possibile il contenuto prima del raggiungimento della quota massima consentita

- Al fine di sfruttare razionalmente lo spazio disponibile per la memorizzazione, ogni utente è soggetto a limiti di utilizzazione; il sistema avvisa l'utente all'approssimarsi del raggiungimento della quota limite impostata. Quando la quota viene superata non è più possibile inviare o ricevere messaggi e archiviare files fino a quando non viene liberato spazio

- È richiesto, nei messaggi in uscita, riportare in calce la firma del soggetto mittente contenente, al minimo: nome, cognome e Settore di appartenenza (quest'ultimo non richiesto per eventuali account di consulenti e collaboratori)

- È necessario porre particolare attenzione ad aprire allegati contenenti programmi "eseguibili" ed accertarsi sempre del mittente. In caso di mittenti dubbi, prima di procedere all'apertura di eventuali allegati, è opportuno condividere con i colleghi del settore la criticità rilevata

- Eventuali messaggi accertati come SPAM o PHISHING devono essere segnalati tramite gli appositi strumenti del proprio account di posta. In caso l'utente rilevi una violazione da parte di malware o ransomware è necessario procedere immediatamente alla disconnessione dalla rete dell'Associazione del dispositivo violato, staccando materialmente il cavo ethernet, disattivando il wifi e spegnendo il dispositivo anche rimuovendo il cavo di alimentazione (in caso di computer portatili dovrà essere rimossa anche la batteria ove possibile)

- È illecito scambiare messaggi sotto falsa identità, ovvero impersonando un altro mittente

- Alla cessazione dell'attività lavorativa, a vario titolo prestata presso l'Associazione, la casella di posta elettronica e lo spazio cloud assegnato all'utente saranno disattivati e successivamente eliminati; è pertanto opportuno salvare o inoltrare ad altri colleghi i messaggi necessari per lo svolgimento delle successive attività lavorative prima della cessazione del rapporto

- La gestione della casella di posta elettronica certificata deve essere effettuata solo dai soggetti individuati dal Dirigente o dalla P.O. di riferimento

USO DELLA RETE LOCALE, INTERNET E RISORSE CONDIVISE

Principi generali

Di norma ogni postazione di lavoro, sia essa di proprietà di Anci Toscana o privata, è connessa alla rete locale dell'Associazione. Agli utenti sono fornite le credenziali per l'accesso agli strumenti di lavoro, ad internet e alle risorse di rete condivise funzionali all'attività lavorativa. Tali accessi devono avvenire esclusivamente per le finalità connesse all'attività di Anci Toscana, strettamente collegate agli incarichi lavorativi.

Regole di utilizzo

Per l'uso dei servizi connessi ad internet, alla rete locale e alle risorse di rete condivise, valgono le seguenti norme comportamentali:

- Non è consentito navigare in internet in siti non attinenti alle attività dell'Associazione
- Non trasferire sulla propria postazione di lavoro, mediante download, file o programmi da siti sconosciuti
- Non scaricare e/o scambiare materiale protetto da diritti di proprietà intellettuale senza averne titolo; nel caso questo avvenga deve sempre essere solo per attività connesse alle esigenze lavorative
- Non è consentito l'uso di programmi *peer to peer* per lo scambio di file in ambito privato
- Non pubblicare testi, immagini o video a contenuto blasfemo, osceno o diffamatorio
- È vietata ogni forma di registrazione a nome dell'Associazione o fornendo i dati relativi ad e-mail di Anci Toscana per l'apertura di account collegati a siti i cui contenuti non siano legati all'attività lavorativa
- Cercare di limitare, ogni volta che sia possibile, le stampe in modo da risparmiare preziose risorse e non intralciare il lavoro altrui
- Il materiale scaricato non pertinente all'attività lavorativa non può essere archiviato nè sullo spazio cloud assegnato, nè sulle cartelle di rete condivise. Sulle unità di rete condivise vengono svolte regolari attività di controllo, amministrazione e backup da parte dei fornitori addetti alla manutenzione; in caso di perdita dei dati è possibile rivolgersi al Dirigente o alla propria P.O. di riferimento per attivare la procedura di recupero dei dati mancanti

CESSAZIONE DEL RAPPORTO DI LAVORO

Al momento della cessazione del rapporto di lavoro o del contratto in essere, o a seguito di qualunque evento che comporti la modifica delle funzioni precedentemente espletate, l'utente deve mettere a disposizione di Anci Toscana tutte le risorse assegnate, sia in termini di attrezzature informatiche che di informazioni di interesse per l'Associazione.
La fase di cessazione prevede le seguenti modalità operative:

- Le credenziali fornite all'utente verranno disabilitate. Sarà cura del Dirigente o della P.O. di riferimento attivare la procedura per la cessazione degli utenti

- La casella di posta elettronica individuale verrà disattivata e successivamente cancellata. Le attività necessarie per il passaggio delle consegne e l'eventuale copia del materiale di interesse dell'Associazione dovranno essere effettuati dall'utente prima della disattivazione

- Le eventuali registrazioni su siti e sistemi esterni, effettuate per motivi di servizio e legate alla casella di posta elettronica dell'utente, dovranno essere portate a conoscenza del Dirigente o della P.O. di riferimento in tempo utile per consentire una loro migrazione verso altri utenti

- Le informazioni e i documenti prodotti o entrati nella disponibilità dell'utente nell'esercizio dell'attività lavorativa restano nella piena ed esclusiva disponibilità di Anci Toscana. L'utente non può fornire, ottenere copia e/o cancellare documenti ed informazioni di interesse dell'Associazione presenti sulle postazioni di lavoro o sulle risorse di rete, né farne alcun uso dopo la cessazione del rapporto di lavoro, o del contratto in essere, a meno di esplicita autorizzazione scritta preventiva da parte del responsabile di Settore o del Dirigente

- Le informazioni eventualmente lasciate sulle postazioni di lavoro o sulle risorse di rete che non siano di interesse per l'Associazione verranno cancellate al termine del rapporto di lavoro, o del contratto in essere, senza alcuna responsabilità per Anci Toscana

CONTROLLI

Eventuali controlli potranno essere effettuati in conformità alla legge, nel rispetto dei principi di necessità, pertinenza e non eccedenza, per verificare le funzionalità e gli aspetti di sicurezza dei sistemi. In caso di abusi singoli o reiterati verranno inoltrati preventivi avvisi collettivi o individuali.

- Anci Toscana, utilizzando sistemi informativi per esigenze produttive o organizzative (ad esempio per rilevare anomalie o per manutenzione), può avvalersi nel rispetto dell'art. 4 comma 2 dello Statuto dei Lavoratori, di sistemi che permettano un controllo indiretto a distanza (controllo preterintenzionale) e determinano un trattamento di dati riferiti o riferibili ai lavoratori, nel rispetto delle "Linee guida del Garante per posta elettronica e internet" emesse dall'Autorità Garante per la protezione dei dati personali il 1 marzo 2007

- Anci Toscana **NON effettua, in alcun caso**, trattamenti di dati personali mediante sistemi informatici che mirino al controllo a distanza dei lavoratori, grazie ai quali sia possibile ricostruire la loro attività e che vengano svolti con i seguenti mezzi:

» Lettura e registrazione sistematica dei messaggi di posta elettronica, al di là di quanto tecnicamente necessario per fornire il servizio di posta stesso
» Memorizzazione ed eventuale riproduzione delle pagine web visitate dal dipendente;
» Lettura e registrazione dei caratteri inseriti dai lavoratori mediante tastiera
» Analisi occulta di computer affidati in uso

- Le attività di controllo, legittimamente svolte da Anci Toscana ai sensi del presente disciplinare, si attengono in ogni caso ai principi fondamentali di finalità e correttezza. I trattamenti sono effettuati per finalità determinate, esplicite e legittime

- Le finalità perseguite da Anci Toscana riguardano o possono riguardare, caso per caso:
» sicurezza sul lavoro
» sicurezza dei sistemi e relativa risoluzione di problemi tecnici
» esigenze di organizzazione
» esigenze di produzione
» rispetto di obblighi legali
» tutela dell' Associazione

- I dati personali contenuti nei log possono essere trattati in forma non anonima solo in via eccezionale ed esclusivamente nelle ipotesi in cui si rilevino evidenze di un utilizzo improprio o illegale, ovvero sia necessario corrispondere ad eventuali richieste della polizia postale e/o dell'autorità giudiziaria

- I dati contenuti nei log sono conservati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di sicurezza – comunque non superiore a sei mesi – e sono cancellati periodicamente ed automaticamente dal sistema

SANZIONI

L'inosservanza delle norme comportamentali descritte nel presente documento può comportare l'applicazione di sanzioni disciplinari, laddove applicabili, ovvero di altre misure di tutela dell'Associazione che si rendessero necessarie.

INFORMATIVA

Anci Toscana assicura al presente Disciplinare ed ai suoi successivi aggiornamenti la più ampia diffusione presso il personale dipendente, i collaboratori, i consulenti, e coloro che a vario titolo prestano servizio o attività per conto e nelle strutture dell'Associazione, mediante:

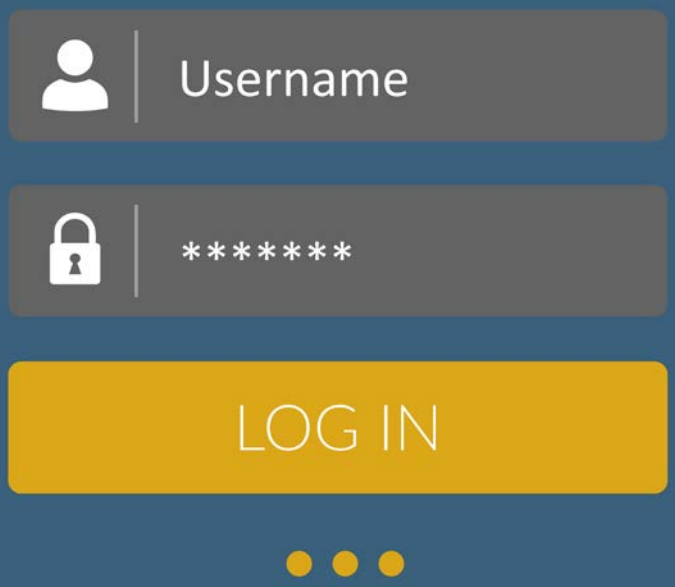
» pubblicazione su file drive condiviso a livello di dominio workspace Anci Toscana
» comunicazione del testo attraverso mailing list dedicate
» trasmissione del testo alle RSU
» trasmissione del regolamento a tutti i futuri dipendenti e a coloro che a vario titolo presteranno servizio o attività per conto e nelle strutture dell'Associazione
» pubblicazione del testo sul sito istituzionale e sul Portale Trasparenza dell'Associazione

CLAUSOLA DI REVISIONE

Il presente Disciplinare è aggiornato periodicamente in relazione all'evoluzione tecnologica, organizzativa e della normativa di settore.

Disciplinare adottato il 19 ottobre 2021

GPDP
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI



Suggerimenti per creare e gestire password a prova di privacy

IMPOSTA BENE LA TUA PASSWORD

Una buona password:

- **deve essere abbastanza lunga**: almeno 8 caratteri, anche se più aumenta il numero dei caratteri più la password diventa "robusta" (si suggerisce intorno ai 15 caratteri);
- **deve contenere caratteri di almeno 4 diverse tipologie**, da scegliere tra: lettere maiuscole, lettere minuscole, numeri, caratteri speciali (cioè punti, trattino, underscore, ecc.);
- **non deve contenere riferimenti personali facili da indovinare** (nome, cognome, data di nascita, ecc.). Non deve nemmeno contenere riferimenti al nome utente (detto anche user account, alias, user id, user name);
- **meglio evitare che contenga parole "da dizionario",** cioè parole intere di uso comune: è meglio usare parole di fantasia oppure parole "camuffate" per renderle meno comuni, magari interrompendole con caratteri speciali (ad esempio: caffè può diventare caf-f3). Esistono infatti software programmati per tentare di indovinare e rubare le password provando sistematicamente tutte le parole di uso comune nelle varie lingue, e con questa accortezza si può rendere il loro funzionamento più complicato;
- **andrebbe periodicamente cambiata**, soprattutto per i profili più importanti o quelli che usi più spesso (e-mail, e-banking, social network, ecc.).

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

GESTISCI BENE LE TUE PASSWORD

- **Utilizza password diverse per account diversi** (e-mail, social network, servizi digitali di varia natura, ecc.). In caso di «furto» di una password si evita così il rischio che anche gli altri profili che ti appartengono possano essere facilmente violati.
- Altra accortezza importante è quella di **NON utilizzare password già utilizzate in passato**.
- Occorre poi ricordare che le eventuali **password temporanee** rilasciate da un sistema o da un servizio informatico vanno sempre immediatamente cambiate, scegliendone una personale.

SE VUOI STARE PIU' TRANQUILLO

Utilizza (laddove disponibili) **meccanismi di autenticazione multi fattore** (es. codici OTP one-time-password), che rafforzano la protezione offerta dalla password.

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

CONSERVA CON CURA LE TUE PASSWORD

- **Non scrivere mai le password su biglietti** che poi magari conservi nel portafoglio o indosso, o che puoi distrattamente lasciare in giro, oppure in file non protetti sui tuoi dispositivi personali (computer, smartphone o tablet).
- **Evita sempre di condividere le password** via e-mail, sms, social network, instant messaging, ecc.. Anche se le comunichi a persone conosciute, le credenziali potrebbero essere diffuse involontariamente a terzi o «rubate» da malintenzionati.
- Se usi pc, smartphone e altri dispositivi che non ti appartengono, **evita sempre che possano conservare in memoria le password da te utilizzate**.

VALUTA SE USARE «GESTORI DI PASSWORD»

Si tratta **di programmi specializzati che generano password sicure** e consentono di appuntare in formato digitale tutte le password salvandole in un database cifrato sicuro. Ce ne sono di vario tipo, gratuiti o a pagamento.

La scheda ha finalità meramente divulgative e sarà aggiornata in base agli sviluppi tecnologici e normativi