DISCIPLINARE INTERNO SULL'USO DI INTERNET, POSTA ELETTRONICA E ALTRI STRUMENTI INFORMATICI

Approvato con Determina del Direttore Generale n. 6 del 22.01.2024

INTRODUZIONE

L'Autorità mette a disposizione del proprio personale dipendente e di eventuali collaboratori esterni i seguenti strumenti di lavoro, in funzione del loro ruolo e delle esigenze lavorative:

- strumenti di informatica individuale, quali personal computer e relativi accessori, ecc;
- apparati e servizi condivisi, quali ad esempio, posta elettronica, internet, stampanti e multifunzioni di rete, file server, ecc;
- programmi e procedure gestionali.

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

Il presente documento illustra le norme generali di utilizzo di tali strumenti che il personale e i collaboratori devono rispettare al fine di mitigare i rischi che un uso improprio degli stessi può determinare alla sicurezza del patrimonio informativo e all'immagine dell'Ente, nonché l'ambito di eventuali verifiche effettuate dal personale addetto riguardo alla funzionalità e sicurezza dei propri sistemi informativi.

Nella stesura del presente documento si è tenuto conto di quanto previsto dalla normativa vigente in materia e, in particolare:

- Regolamento UE 2016/679 e successiva regolamentazione con D. Lgs. 101/2018,
- provvedimenti emessi dall'Autorità Garante per la protezione dei dati personali, in particolare il provv. 1° marzo 2017 "*Linee guida del Garante per posta elettronica e internet*",
- circolari dell'Agenzia per l'Italia Digitale (AGID), in particolare la circ. 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)*";
- 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);
- DPR 81/2023 ad oggetto "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*";

L'Autorità non effettua registrazioni per il controllo dell'attività lavorativa dei dipendenti, ma solo registrazioni volte a salvaguardare la sicurezza ed il mantenimento dell'efficienza dei sistemi. I dati registrati automaticamente a tale scopo non vengono utilizzati in alcun modo per il controllo a distanza dei lavoratori e le tecnologie utilizzate a tal fine sono compatibili con quanto disposto dalla normativa vigente in materia.

AMBITO DI APPLICAZIONE

Le disposizioni contenute nel presente documento si applicano a tutti i dipendenti dell'Autorità nonché a tutti i soggetti esterni ai quali verranno espressamente riconosciute applicabili (ad esempio collaboratori esterni).

È responsabilità di tutti i soggetti che utilizzano la strumentazione informatica, la posta elettronica e internet messi a disposizione dall'Autorità, applicare e rispettare puntualmente le disposizioni del presente Disciplinare.

AVVIO DEL RAPPORTO DI LAVORO E CAMBIAMENTI DI MANSIONE

In occasione dell'entrata in servizio di un/a nuovo/a dipendente, il Dirigente/Responsabile del Servizio a cui afferisce la risorsa richiede all'Amministratore di Sistema il rilascio delle credenziali per l'accesso ai sistemi informativi dell'Ente e alla casella di posta elettronica.

Il suddetto Dirigente/Responsabile comunica inoltre all'Amministratore di Sistema il ruolo del lavoratore per la corretta configurazione dei diritti di accesso, anche in riferimento ai trattamenti dati da esso/a effettuati (a tal fine devono essere indicati all'Amministratore di Sistema le risorse informatiche che il dipendente deve utilizzare per lo svolgimento dei propri compiti lavorativi).

Analogamente, in caso di cambiamento di mansione o di trasferimento tra Servizi, il Dirigente/ Responsabile di Servizio a cui afferisce la risorsa comunica il cambiamento all'Amministratore di Sistema, indicando il nuovo ruolo ai fini della corretta configurazione dei diritti di accesso.

UTILIZZO DELLE POSTAZIONI DI LAVORO

In funzione del proprio ruolo e delle esigenze organizzative e lavorative, il personale in servizio presso l'Autorità è dotato di personal computer e/o altri dispositivi per lo svolgimento di attività connesse agli incarichi lavorativi, nel rispetto delle regole di seguito descritte.

Il personal computer e gli eventuali altri dispositivi, di cui l'Ente è esclusiva proprietaria, sono assegnati nominalmente al dipendente e sono a tutti gli effetti uno strumento di lavoro. Ognuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione dall'Autorità.

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.
L'Ente, anche ai fini della gestione delle assenze prolungate e delle cessazioni, promuove l'utilizzo condiviso delle informazioni; a tale fine i dipendenti utilizzano cartelle di lavoro condivise con il personale del proprio Servizio/Ufficio o di altre strutture organizzative in considerazione della materia trattata, messe a disposizione dall'Amministratore di Sistema.

In ogni caso il dipendente si attiene alle seguenti disposizioni:

a) utilizzare il computer, le stampanti e comunque tutte le dotazioni di lavoro assegnate in modo da salvaguardarne l'integrità e il corretto funzionamento e non per fini personali;
b) non installare o eseguire autonomamente programmi esterni senza l'esplicita autorizzazione dell'Amministratore di Sistema al fine di prevenire il pericolo di importare virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore. Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dall'Ente. L'inosservanza di questa disposizione, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'Ente a responsabilità civili e penali in caso di violazione della normativa a tutela dei diritti d'autore sul software. In merito si precisa che anche il software freeware spesso è tale solo per uso personale e non aziendale e pertanto soggetto a licenza d'acquisto;
c) non lasciare incustodita la sessione di lavoro avendo cura di "*spegnere*" il computer o "*disconnettere*" la propria utenza al termine del proprio orario di lavoro; in caso di allontanamento temporaneo è necessario, fatti salvi i casi di urgenza, disconnettere la propria utenza o comunque rendere la postazione di lavoro inaccessibile ad estranei;
d) è cura degli utilizzatori provvedere alla archiviazione periodica dei dati (non dei programmi): si sottolinea che i dati sono di proprietà dell'Ente e non personale e che la perdita degli stessi può causare grave danno all'Amministrazione la cui responsabilità ricade sull'utilizzatore. A tale proposito si raccomanda di non salvare i dati di lavoro sul proprio computer locale ma di assicurarsi che i file sui quali si lavora siano archiviati sulle risorse condivise del server dell'Ente;
e) è cura dell'utilizzatore proteggere tramite criptazione i file contenenti dati personali (dati comuni, categorie particolari di dati e dati giudiziari), salvati sul proprio computer locale;
f) non è consentito all'utente modificare le caratteristiche di sistema (nome computer, indirizzi IP, DNS, Firewall, aggiornamenti automatici SW, etc.);
g) non è consentito connettere alla rete dell'Ente computer portatili personali o di terzi in maniera autonoma senza previa autorizzazione dell'Amministratore di Sistema. L'inosservanza di tale norma può essere causa di gravi rischi alla sicurezza e alla funzionalità dei sistemi informativi dell'Ente;

h) non è consentita l'installazione sul PC utilizzato di nessun dispositivo di comunicazione (come adesempio modem, ecc.), se non con l'autorizzazione espressa dell'Amministratore di Sistema;
i) è consentito l'utilizzo di chiavette USB o dischi esterni (vedi paragrafo "Utilizzo supporti esterni); in tal caso è responsabilità dell'utilizzatore far sì che tale uso noncompromette la sicurezza del sistema informativo dell'Ente.
j) non è consentito masterizzare cd e dvd per finalità personali;
k) cancellare i file di lavoro nelle aree condivise del server dedicate a contenere file temporanei non appena abbiano esaurito la loro funzione;
l) informare tempestivamente l'Ente e l'Amministratore di sistema sui potenziali rischi o problemi inerenti alla sicurezza informatica della propria postazione di lavoro.
m) in caso di smarrimento o furto di dispositivi informatici, oltre a sporgere regolare denuncia all'autorità competente, informare tempestivamente l'Amministratore di Sistema ed il proprio Dirigente o Responsabile di Servizio comunicando quali dati erano contenuti all'interno;

Ai soli fini di prestare assistenza tecnica ai dipendenti o di garantire la sicurezza dei sistemi informativi dell'Ente, l'Amministratore di sistema può utilizzare software o strumenti che consentano di operare sulla postazione di lavoro del dipendente in remoto. Tali attività possono essere svolte solo per il tempo strettamente necessario alla risoluzione della problematica riscontrata e comunque sono sottoposte al preventivo consenso del dipendente; nei casi urgenti l'Amministratore di sistema dovrà, comunque, fornire al dipendente tempestiva comunicazione dell'avvenuto accesso.

UTILIZZO DELLE POSTAZIONI DI LAVORO MOBILI

L'Ente consegna a specifici dipendenti personal computer portatili. Le regole di utilizzo di queste apparecchiature sono le stesse dei personal computer collegati alla rete locale con particolare riguardo alla criptazione dei file contenenti dati personali.

Il loro utilizzo richiede inoltre maggiori precauzioni rispetto alle postazioni fisse in ordine ai seguenti elementi:

- verificare la presenza di tutte le misure atte ad evitare l'accesso ai dati personali eventualmente contenuti in caso di furto o acquisizioni indebite da parte di terzi non autorizzati;

- l'interessato è responsabile del pc portatile assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro;

- i computer portatili utilizzati all'esterno (in occasione di convegni, corsi, trasferte, ecc.), in caso di allontanamento, devono essere custoditi in un luogo protetto;
- al fine di prevenirne il furto, è vietato lasciare i computer portatili in luoghi non opportunamente custoditi;
- è vietato far utilizzare il proprio computer portatile assegnato in dotazione a soggetti terzi;
- informare tempestivamente l'Ente e l'Amministratore di sistema su potenziali rischi o problemi inerenti alla sicurezza informatica del portatile;

È quindi a carico dell'utilizzatore garantire la funzionalità e l'aggiornamento del sistema.

Per quanto riguarda i dispositivi che contengono certificati di firma dei titolari, utilizzabili ad esempio nei procedimenti amministrativi dell'Ente, i destinatari sono responsabili del corretto utilizzo e devono custodire adeguatamente i dispositivi, il relativo PIN e altro materiale a corredo.

UTILIZZO DI SUPPORTI ESTERNI

Di seguito le regole da rispettare in caso di utilizzo di supporti esterni:

- Tutti i supporti esterni (CD, DVD, supporti di memorizzazione USB, HD esterni) contenenti dati dell'Ente devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere acquisito indebitamente da personale non autorizzato;
- i supporti esterni contenenti dati personali che rientrino nelle categorie particolari ex artt. 9 e 10 GDPR 2016/679 (es. idonei a rivelare lo stato di salute, ecc.) devono essere custoditi in archive dotati di serratura;
- è cura dell'utilizzatore proteggere tramite criptazione i file contenenti dati personali salvati sul supporto esterno;
- è vietato smaltire supporti di memorizzazione esterna, anche se non funzionanti se non nelrispetto delle disposizioni impartite dall'Ente;
- è consentito l'utilizzo di chiavette USB o dischi esterni demandando all'utilizzatore che tale uso non comprometta la sicurezza del sistema informativo dell'Ente.
- è assolutamente vietato utilizzare chiavette USB trovate casualmente (per la strada, vicino lapropria abitazione, ufficio, parcheggio, ecc.);
- garantire sui supporti removibili tutte le misure atte ad evitare furti e acquisizione indebite da parte di terzi non autorizzati;
- verificare la presenza di tutte le misure atte ad evitare l'accesso ai dati personali eventualmente contenuti in caso di furto e acquisizioni indebite da parte di terzi non autorizzati;

- eventuali supporti esterni contenenti informazioni di lavoro di proprietà dell'Ente devono essere prontamente riconsegnati all'Ente medesimo al termine del rapporto di lavoro/incarico;
- informare tempestivamente l'Ente e l'Amministratore di sistema su potenziali rischi o problemi inerenti alla sicurezza informatica dei supporti removibili utilizzati.

UTILIZZO DELLE CARTELLE CONDIVISE

L'Ente organizza i file di lavoro su file server tramite la condivisione di cartelle. Le cartelle sono organizzate in parte in base alle mansion attribuite a ciascun dipendente e in parte in base a gruppi di lavoro trasversali alle aree/servizi/uffici. Ciascun utente è tenuto a utilizzare le cartelle in modo coerente con il procedimento a cui sta lavorando, avendo cura di salvare i dati in cartelle dove abbiano accesso solo le persone autorizzate al loro trattamento. Ciascun Dirigente/Responsabile di Servizio organizzerà i contenuti della cartella riguardante la propria Area/Servizio e avrà cura di comunicare ai propri collaboratori la corretta modalità di collocazione dei file.

UTILIZZO DEL TELEFONO AZIENDALE

I telefoni "fissi" e i cellulari aziendali, che l'Ente mette a disposizione dei suoi dipendenti, devono essere utilizzati in modo strettamente pertinente allo svolgimento dell'attività lavorativa, secondo un utilizzo appropriato, efficiente, corretto e razionale.

Solo in caso di particolare necessità e/o urgenza, i dipendenti possono utilizzare tali beni per motivi personali non attinenti all'attività lavorativa e, comunque, non in modo ripetuto o per periodi di tempo prolungati, salvo i casi appositamente autorizzati dall'Ente.

CREDENZIALI E PASSWORD

Le credenziali (nome utente e password) per l'accesso alla rete, al dominio, alla posta ed ai personal computer vengono rilasciate dall'Amministratore di Sistema previa richiesta da parte del Dirigente/Responsabile di Servizio dell'utente interessato, con contestuale fornitura dei dati identificativi necessari alla creazione.
Le credenziali di accesso alle singole procedure (protocollo, contabilità, ecc.) vengono rilasciate solo

dopo aver ricevuto preventiva autorizzazione scritta da parte del Dirigente/Responsabile del Servizio titolare della procedura (ad esempio Dirigente Area Amministrativa e Contabile per il programma protocollo e contabilità, ecc).
L'Amministratore di Sistema provvede inoltre, a rigenerare password scadute o dimenticate ed a disattivare le utenze cessate.
L'utente deve essere consapevole del fatto che cedere le proprie credenziali, ovvero permettere a terzi l'accesso ai servizi comunali, significa autorizzarli a proprio nome alla gestione degli stessi, con effetti potenzialmente gravissimi (ad es. visualizzazione di informazioni riservate, alterazione o distruzione di dati, abuso della propria posta elettronica); inoltre questo comportamento può esporlo a responsabilità civile e penale per eventuali utilizzi illeciti.
Per una corretta gestione delle credenziali di autenticazione è necessario osservare le seguenti regole:

- modificare alla prima connessione la password che l'Amministratore di Sistema attribuisce e comunica;
- usare, nella composizione della password, almeno 8 caratteri, di cui almeno un carattere numerico e uno speciale, e non basarla su informazioni facilmente deducibili, quali il proprio nome, il nome dei familiari, la data di nascita, il codice fiscale;
- modificare la password ogni volta che il sistema in modo automatico richiede l'aggiornamento e nel caso in cui si ritenga che la propria password sia stata compromessa, modificarla immediatamente;
- mantenere la password riservata, non lasciarla incustodita o in vista sulla propria postazione di lavoro, non divulgarla 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;
- non trascriverla su supporti facilmente accessibili a terzi (ad es. foglietti, post-it, ecc.);
- non permettere ad altri utenti o colleghi di operare con le proprie credenziali;

USO DELLA POSTA ELETTRONICA

La Posta Elettronica che l'Ente mette a disposizione dei suoi dipendenti deve essere utilizzata in modo pertinente allo svolgimento dell'attività lavorativa, secondo un utilizzo appropriato, efficiente, corretto e razionale nel rispetto del principio di riservatezza. Il data base della posta elettronica è di esclusiva proprietà dell'Ente che vi può accedere per motivi tecnici e di sicurezza nel rispetto della normativa vigente.

Per l'utilizzo della posta elettronica il dipendente deve attenersi alle seguenti norme comportamentali:

- l'uso della posta elettronica istituzionale è consentito esclusivamente per motivi attinenti

allo svolgimento delle mansioni assegnate, l'utente del servizio è consapevole che i contenuti della posta elettronica dell'Ente non devono avere carattere privato o personale, ma devono riguardare esclusivamente questioni connesse all'attività lavorativa; l'uso della posta elettronica istituzionale non può in alcun modo compromettere la sicurezza o la reputazione dell'amministrazione;

- L'utilizzo di caselle di posta elettroniche personali è di norma evitato per attività o comunicazioni afferenti al servizio, salvi i casi di forza maggiore dovuti a circostanze in cui il dipendente, per qualsiasi ragione, non possa accedere all'account istituzionale;
- il titolare di indirizzo di posta elettronica ha il dovere di controllare periodicamente la propria casella elettronica, verificare l'arrivo di nuovi messaggi, cancellare i messaggi obsoleti o inutili, verificare lo spazio occupato, prestare attenzione ai messaggi di quota raggiunta, ripulire la casella di posta prima del raggiungimento della quota massima consentita;
- è richiesto, nei messaggi in uscita, riportare in calce la firma del soggetto mittente contenente, al minimo: nome, cognome, Servizio di appartenenza e recapito istituzionale;
- dato il carattere istituzionale delle caselle di posta è fatto divieto inoltrare all'esterno messaggi non inerenti alle proprie competenze nell'Ente ed utilizzare l'indirizzo di posta per motivi non legati all'attività lavorativa ed istituzionale;
- in caso di assenza prolungata programmata del dipendente, si consiglia e si raccomanda di attivare il sistema di risposta automatica ai messaggi di posta elettronica ricevuti indicando, nel messaggio di accompagnamento, l'indirizzo del Servizio di riferimento che può essere contattato in sua assenza;
- è obbligatorio controllare i file allegati di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti);
- non partecipare a c.d. "*catene di s. Antonio*" e simili;
- salvo espressa autorizzazione da parte dell'Amministrazione, non è consentito il "*redirect*" della propria casella di posta di lavoro su e-mail personali;
- è assolutamente vietato aprire allegati di e-mail di provenienza dubbia che fanno riferimento ad acquisti di e-commerce, corrieri per il ritiro di materiale o fantomatici rimborsi;
- informare tempestivamente l'Ente e l'Amministratore di Sistema su potenziali rischi o problemi inerenti alla sicurezza informatica della posta elettronica;
- è vietato l'invio di messaggi di posta elettronica, all'interno o all'esterno dell'amministrazione, che siano oltraggiosi, discriminatori o che possano essere in qualunque modo fonte di responsabilità dell'amministrazione;
- alla cessazione dell'attività lavorativa presso l'Autorità, la casella di posta elettronica del dipendente sarà disattivata e successivamente eliminata, è pertanto opportuno salvare o

inoltrare ad altri i messaggi che fossero necessari per le successive esigenze lavorative del servizio prima delle dimissioni.

UTILIZZO DI INTERNET

Le postazioni di lavoro dell'Ente consentono la connessione alla rete Internet oltre che a quella intranet ed alle risorse condivise. Tali accessi devono avvenire per finalità istituzionali connesse alle attività lavorative svolte e nel rispetto del presente Disciplinare.

Fatta salva la possibilità per i dipendenti di utilizzare la rete Internet per assolvere ad incombenze personali di natura amministrativa o burocratica, purché l'attività sia contenuta in tempi ristretti e senza alcun pregiudizio per i compiti istituzionali (ad esempio, per effettuare adempimenti on line nei confronti di pubbliche amministrazioni e di concessionari di servizi pubblici, ovvero per tenere rapporti con istituti bancari e assicurativi), non è consentito:

- navigare in siti non attinenti alle mansioni affidate;
- partecipare per motivi non professionali a forum on-line, bacheche elettroniche e guest book anche utilizzando pseudonimi o nickname;
- utilizzare chat line o social network (Facebook, Instagram, Twitter, ecc.);
- registrarsi in siti non attinenti alle attività professionali (newsletter, guest book);
- scaricare software gratuiti senza l'autorizzazione dell'Ente;
- scaricare documenti informatici di natura oltraggiosa o discriminatoria o comunque che possono rivelare opinioni politiche, religiose, sindacali o sessuali;
- scaricare file musicali;
- utilizzare, a meno di esigenze professionali, servizi in streaming audio o video (Internet radio, filmati, YouTube, ecc.) che compromettono la banda disponibile causando perdite di efficienza della rete aziendale;
- accedere a siti che contengono materiale pornografico;
- pubblicare su account personali di social network (es. Facebook, ecc.) fotografie o dati personali riconducibili agli utenti, al personale dell'Ente, e più in generale alle attività svolte nell'Ente;
- scaricare materiale protetto dal diritto d'autore;

Il dipendente deve informare tempestivamente l'Ente e l'Amministratore di Sistema su potenziali rischi o problemi inerenti alla sicurezza informatica relativi agli accessi ad Internet.

SOCIAL NETWORK

L'utilizzo dei social network (Facebook, Twitter, ecc.) deve limitarsi alle attività di diffusione di informazioni riferite all'Ente ed è riservato, di norma, al personale di altri Servizi/Uffici autorizzato,

per finalità istituzionali.
Nell'utilizzo dei propri account di social media, il dipendente utilizza ogni cautela affinché le proprie opinioni o i propri giudizi su eventi, cose o persone, non siano in alcun modo attribuibili direttamente all'Autorità. In ogni caso il dipendente è tenuto ad astenersi da qualsiasi intervento o commento che possa nuocere al prestigio, al decoro o all'immagine dell'Autorità o della pubblica amministrazione in generale.
È vietato postare nel proprio account di Facebook (o similari) fatti, eventi e foto attinenti all'Autorità o comunicare tramite strumenti social (es. Linkedin) informazioni non veritiere sul proprio ruolo lavorativo al fine di trarne un vantaggio in termini di visibilità professionale e personale o altre utilità.
Al fine di garantirne i necessari profili di riservatezza le comunicazioni, afferenti direttamente o indirettamente il servizio non si svolgono, di norma, attraverso conversazioni pubbliche mediante l'utilizzo di piattaforme digitali o social media. Sono escluse da tale limitazione le attività o le comunicazioni per le quali l'utilizzo dei social media risponde ad una esigenza di carattere istituzionale.
I dipendenti non possono divulgare o diffondere per ragioni estranee al loro rapporto di lavoro con l'Autorità e in difformità alle disposizioni di cui al decreto legislativo 13 marzo 2013, n. 33, e alla legge 7 agosto 1990, n. 241, documenti, anche istruttori, e informazioni di cui essi abbiano la disponibilità.

CONTROLLI

Nei casi in cui si renda necessario accedere, mediante strumenti informatici, a dati o informazioni riferiti o riferibili ai propri dipendenti per esigenze istituzionali o per il buon funzionamento e la sicurezza del sistema informativo, l'Ente procede nel rispetto dell'art. 4, comma 2, dello Statuto dei Lavoratori, delle "*Linee guida del Garante per posta elettronica e internet*" emesse dall'Autorità Garante per la protezione dei dati personali il 1° marzo 2007 e del presente Disciplinare.
L'Ente 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.
Le attività di controllo, legittimamente svolte dall'Ente ai sensi del presente Disciplinare, si attengono in ogni caso ai seguenti principi fondamentali:

- Necessità, pertinenza, graduazione e non eccedenza: i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite, osservando altresì, il principio di pertinenza e non eccedenza. L'Ente raccoglie e tratta i dati nella misura meno invasiva possibile; le eventuali attività di controllo sono svolte solo da soggetti preposti;
- Finalità e correttezza: i trattamenti sono effettuati per finalità determinate, esplicite e

legittime. Le finalità perseguite dall'Ente 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'Ente.

Le attività che comportano l'uso del servizio di accesso ad Internet vengono automaticamente filtrate in base a policy di sicurezza stabilite dal Titolare e registrate in forma elettronica localmente oppure può essere affidato ad un fornitore esterno; inoltre sono memorizzate su log di sistema con le sole finalità statistiche sull'utilizzo dell'infrastruttura; Il trattamento dei dati contenuti nei log predetti può avvenire esclusivamente in forma anonima, in modo da precludere l'identificazione degli utenti e delle loro attività.

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 non conforme alle policy di sicurezza, 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.

OBBLIGATORIETÀ E SANZIONI

È fatto obbligo a tutti i dipendenti di osservare le disposizioni di cui al presente Disciplinare.

Il mancato rispetto o la violazione delle regole contenute nel presente Disciplinare è perseguibile con tutte le azioni civili e penali previste dalla legge, nonché con i provvedimenti disciplinari, in conformità a quanto previsto dalle disposizioni normative e contrattuali vigenti per il personale e con tutte le misure di tutela del caso.

CESSAZIONE DEL RAPPORTO DI LAVORO

Al momento della cessazione del rapporto di lavoro, ovvero di qualunque evento che comporti la modifica delle funzioni precedentemente espletate, l'utente deve mettere a disposizione dell'Ente tutte le risorse assegnate, sia in termini di attrezzature informatiche che di informazioni di interesse per i Servizi.

La fase di cessazione prevede le seguenti modalità operative:

- le credenziali fornite all'utente verranno disabilitate entro una settimana: è cura del Dirigente/Responsabile del Servizio interessato comunicare le cessazioni degli utenti

all'Amministratore di Sistema;

- la casella di posta elettronica individuale verrà disattivata entro una settimana e successivamente cancellata (entro 3 mesi): le attività necessarie per il passaggio delle consegne e la copia del materiale di interesse del Servizio/Ufficio dovranno essere effettuati prima della disattivazione, a cura del responsabile del Servizio interessato;
- il lavoratore non può cancellare le informazioni di interesse istituzionale presenti sui sistemi condivisi, senza esplicita autorizzazione dell'Ente;
- le eventuali registrazioni su siti e sistemi esterni, effettuate per motivi di servizio e legate alla casella di posta elettronica del dipendente, dovranno essere portate a conoscenza del Dirigente/Responsabile di Servizio in tempo utile per consentire una loro migrazione verso altri utenti, ovvero la loro disabilitazione;
- le informazioni e i documenti prodotti o entrati nella disponibilità dell'utente nell'esercizio dell'attività lavorativa a favore dell'Autorità restano nella piena ed esclusiva disponibilità dell'Ente;
- l'utente non può formare, ottenere copia e/o cancellare documenti ed informazioni di interesse dell'Autorità, presenti sulle postazioni di lavoro o sulle risorse di rete, né farne alcun uso dopo la cessazione del rapporto di lavoro, a meno di esplicita autorizzazione scritta preventiva da parte del Dirigente/Responsabile di Servizio;
- le informazioni eventualmente lasciate sulle postazioni di lavoro o sulle risorse di rete che non siano di interesse per l'Autorità verranno cancellate al termine del rapporto di lavoro senza alcuna responsabilità per l'Ente.

INFORMATIVA

Il presente Disciplinare costituisce informativa ai sensi del GDPR 2016/679 e della vigente normativa nazionale in materia di privacy circa le modalità e le finalità del trattamento dei dati personali connessi all'uso delle risorse informatiche e dei servizi di rete.

Il presente Disciplinare costituisce altresì informativa ai sensi dell'art. 4, comma 3, della Legge 20 maggio 1970, n. 300 e s.m.i. circa le modalità e finalità del trattamento dei dati personali connessi all'uso delle risorse informatiche e dei servizi di rete.
L'Ente assicura al presente Disciplinare ed ai suoi successivi aggiornamenti la più ampia diffusione, mediante:

- pubblicazione nella rete intranet;
- comunicazione a tutti i dipendenti e a coloro che a vario titolo prestano servizio o attività per conto e nelle strutture dell'Ente;

- comunicazione alla RSU ed alle sigle sindacali firmatarie del Contratto Integrativo Decentrato;
- consegna ai nuovi dipendenti assunti e a coloro che a vario titolo presteranno servizio o attività per conto e nelle strutture dell'Ente;
- pubblicazione in forma permanente sul sito web istituzionale dell'Ente.

Per qualunque informazione gli interessati potranno rivolgersi al Titolare del trattamento dei dati o al Responsabile della protezione dei dati (DPO) - e-mail: pa@privacysolving.it

AGGIORNAMENTO/REVISIONE ED ENTRATA IN VIGORE

Il presente Disciplinare viene aggiornato periodicamente in relazione all'evoluzione tecnologica, alle modifiche normative ed alle disposizioni organizzative dell'Ente.

Il presente Disciplinare entra in vigore il giorno stesso della sua pubblicazione all'Albo Pretorio on line dell'Autorità.

Il Direttore Generale
Ing. Enzo Tacconi (*)

(*) Documento informatico sottoscritto con firma digitale
ai sensi del D.Lgs. 82/2005