fondazione
Banco Napoli
per l'Assistenza
all'Infanzia

AZIENDA PUBBLICA DI SERVIZI PER L'ASSISTENZA ALL'INFANZIA

REGOLAMENTO PER L'UTILIZZO DELLA STRUMENTAZIONE INFORMATICA AZIENDALE E DELLA RETE INTERNET

Approvato con deliberazione del C.d.A. n. 79/2018

Sede: Via Don Bosco, 7 – 80141 Napoli – Tel. 0817511815 – 0817511994 - 0817516326
Fax: 0817518341 – http: www.fbnai.it
Pec: protocollo@pec.fbnai.it – Mail: info@fbnai.it

INDICE

CAPO I – I PRINCIPI

ART. 1
INTRODUZIONE, DEFINIZIONI E FINALITA'

Il presente disciplinare interno ha l'obiettivo di definire l'ambito di applicazione, le modalità e le norme sull'utilizzo della strumentazione informatica da parte degli utenti assegnatari (dipendenti, collaboratori etc.), al fine di tutelare i beni aziendali ed evitare condotte inconsapevoli e/o scorrette che potrebbero esporre la Ente a problematiche di sicurezza, di immagine e patrimoniali per eventuali danni cagionati anche a terzi.
L'insieme delle norme comportamentali ivi incluse, pertanto, è volto a conformare la Ente ai principi di diligenza, informazione e correttezza nell'ambito dei rapporti di lavoro, con l'ulteriore finalità di prevenire eventuali comportamenti illeciti dei dipendenti, pur nel rispetto dei diritti ad essi attribuiti dall'ordinamento giuridico italiano.
A tal fine, pertanto, si rileva che gli eventuali controlli ivi previsti escludono finalità di monitoraggio diretto ed intenzionale dell'attività lavorativa e sono disposti sulla base della vigente normativa, con particolare riferimento al *Regolamento UE n. 2016/679*, alla *Legge n. 300/1970* (c.d. Statuto dei Lavoratori) ed ai provvedimenti appositamente emanati dall'Autorità Garante (si veda in particolare *Provv. 1 marzo 2007*).

ART. 2
AMBITO DI APPLICAZIONE

Il presente disciplinare interno si applica ad ogni *Utente* assegnatario di beni e risorse informatiche aziendali ovvero utilizzatore di servizi e risorse informative di pertinenza dell'Ente.
Per *Utente* si intende, pertanto, a titolo esemplificativo e non esaustivo, ogni presente, collaboratore (interno o esterno), presente, fornitore e/o terzo che in modo continuativo e non occasionale operi all'interno della struttura aziendale utilizzandone beni e servizi informatici.
Per *Ente* si intende, invece, l'Ente, l'organizzazione e/o comunque il Titolare dei beni e delle risorse informatiche ivi disciplinate, il quale opererà per mezzo dei soggetti che ne possiedono la rappresentanza.

ART. 3
TITOLARITA' DEI BENI E DELLE RISORSE INFORMATICHE

I beni e le risorse informatiche, i servizi ICT e le reti informative costituiscono beni aziendali rientranti nel patrimonio sociale e sono da considerarsi di esclusiva proprietà della Ente.
Il loro utilizzo, pertanto, è consentito solo per finalità di adempimento delle mansioni lavorative affidate ad ogni Utente in base al rapporto in essere (ovvero per scopi professionali afferenti l'attività svolta per l'Ente), e comunque per l'esclusivo perseguimento degli obiettivi aziendali.
A tal fine si precisa sin d'ora che qualsivoglia dato e/o informazione trattato per mezzo dei beni e delle risorse informatiche di proprietà dell'Ente, sarà dallo stesso considerato come avente natura aziendale e non riservata.

ART. 4
RESPONSABILITA' PERSONALE DELL'UTENTE

Ogni Utente è personalmente responsabile dell'utilizzo dei beni e delle risorse informatiche affidatigli dalla Ente nonché dei relativi dati trattati per finalità aziendali.

A tal fine ogni Utente, nel rispetto dei principi di diligenza sottesi al rapporto instaurato con l'Ente, è tenuto a tutelare (per quanto di propria competenza) il patrimonio aziendale da utilizzi impropri e non autorizzati, danni o abusi anche derivanti da negligenza, imprudenza o imperizia. L'obiettivo è quello di preservare l'integrità e la riservatezza dei beni, delle informazioni e delle risorse aziendali.
Ogni Utente, pertanto, è tenuto, in relazione al proprio ruolo e alle mansioni in concreto svolte, ad operare a tutela della sicurezza informatica aziendale, riportando al proprio responsabile e senza ritardo eventuali rischi di cui è a conoscenza ovvero violazioni del presente disciplinare interno.
Sono vietati comportamenti che possano creare un danno, anche di immagine, alla Ente.

ART. 5
I CONTROLLI

I principi

L'Ente, in linea con quanto prescritto dall'ordinamento giuridico italiano (art. 4, Statuto dei Lavoratori), esclude la configurabilità di forme di controllo aziendali aventi direttamente ad oggetto l'attività lavorativa dell'Utente.
Ciononostante non si esclude che, per ragioni organizzative e produttive ovvero per esigenze dettate dalla sicurezza del lavoro, si utilizzino sistemi informatici, impianti o apparecchiature dai quali derivi la possibilità di controllo a distanza dell'attività dei lavoratori.
In tali casi, infatti, sarà onere della Ente sottoporre tali forme di controllo all'accordo con le rappresentanze sindacali aziendali ovvero, in assenza di queste, con la commissione interna. In difetto di accordo, su istanza della Ente, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti.
I controlli posti in essere, pertanto, saranno sempre tali da evitare ingiustificate interferenze con i diritti e le libertà fondamentali dei lavoratori e non saranno costanti, prolungati e indiscriminati.
L'Ente, nel riservarsi il diritto di procedere a tali controlli sull'effettivo adempimento della prestazione lavorativa nonché sull'utilizzo da parte degli utenti dei beni e dei servizi informatici aziendali (artt. 2086, 2087 e 2104 c.c.), agirà in base al principio della "*gradualità*".
Secondo questo principio:

- I controlli saranno effettuati inizialmente solo su dati aggregati riferiti all'intera struttura aziendale ovvero a singole aree lavorative.
- Nel caso in cui si dovessero riscontrare violazioni del presente disciplinare interno, indizi di commissione di gravi abusi o illeciti o attività contrarie ai doveri di fedeltà e diligenza, verrà diffuso un avviso generalizzato, o circoscritto all'area o struttura lavorativa interessata, relativo all'uso anomalo degli strumenti informatici aziendali, con conseguente invito ad attenersi scrupolosamente alle istruzioni ivi impartite.
- In caso siano rilevate ulteriori violazioni, si potrà procedere con verifiche più specifiche e puntuali, anche su base individuale.

I controlli non autorizzati

In ogni caso la Ente non può in alcun caso utilizzare sistemi da cui derivino forme di controllo a distanza dell'attività lavorativa che permettano di ricostruire l'attività del lavoratore.
Per tali s'intendono, a titolo meramente esemplificativo e non esaustivo:

- la lettura e la registrazione sistematica dei messaggi di posta elettronica, al di là di quanto necessario per fornire e gestire il servizio di posta elettronica stesso;
- la memorizzazione sistematica delle pagine internet visualizzate da ciascun Utente, dei contenuti ivi presenti, e del tempo di permanenza sulle stesse;
- la lettura e la registrazione dei caratteri inseriti dal lavoratore tramite tastiera o dispositivi analoghi;
- l'analisi dei dispositivi per l'accesso alla rete internet.

CAPO II – MISURE ORGANIZZATIVE

ART. 6
AMMINISTRATORI DEL SISTEMA

L'Ente conferisce all'amministratore di sistema il compito di sovrintendere i beni e le risorse informatiche aziendali.
È compito dell'amministratore di sistema:

1) gestire l'hardware e il software di tutta la strumentazione informatica di appartenenza dell'Ente;
2) gestire la creazione, l'attivazione, la disattivazione, e tutte le relative attività amministrative degli account di rete e dei relativi privilegi di accesso alle risorse, previamente assegnati agli utenti;
3) monitorare il corretto utilizzo delle risorse di rete, dei computer e degli applicativi affidati agli utenti, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza, e della protezione dei dati;
4) creare, modificare, rimuovere o utilizzare qualunque account o privilegio purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza, e della protezione dei dati;
5) rimuovere software e/o componenti hardware dalle risorse informatiche assegnate agli utenti, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza, e della protezione dei dati;
6) provvedere alla sicurezza informatica dei sistemi informativi aziendali, nel rispetto di quanto prescritto dal GDPR 679/2016 (art.32);
7) provvedere ad effettuare copie di backup dei supporti contenenti dati;
8) utilizzare le credenziali di accesso di amministratore del sistema per accedere, anche da remoto, ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un Utente in caso di prolungata assenza, irrintracciabilità o impedimento dello stesso. Tale ultima attività, tuttavia, deve essere disposta per mezzo di un soggetto che rivesta quantomeno la posizione di responsabile privacy all'interno della Ente e deve essere limitata altresì al tempo strettamente necessario al compimento delle attività indifferibili per cui è stato richiesto.

Tutto ciò premesso sono designati soggetti con competenza specifica.
Di seguito si riportano i nominativi degli amministratori di sistema dell'Ente:
- Francesco Iacomino.

ART. 7
ASSEGNAZIONE DEGLI ACCOUNT E GESTIONE DELLE PASSWORD

Creazione e gestione degli Account
Un account Utente consente l'autenticazione dell'utilizzatore e di conseguenza ne disciplina l'accesso alle risorse informatiche aziendali, per singola postazione lavorativa.
Gli account utenti vengono creati dagli amministratori di sistema e sono personali, ovvero associati univocamente alla persona assegnataria.
L'accesso al proprio account avviene tramite l'utilizzo delle "credenziali di autenticazione" (es. "Username" e "Password"), comunicate all'Utente dall'amministratore di sistema, che le genera, attraverso modalità che ne garantiscano la segretezza (Es: busta chiusa e sigillata).

Le credenziali di autenticazioni costituiscono dati aziendali da mantenere strettamente riservati e non è consentito comunicarne gli estremi a terzi (seppur soggetti in posizione apicale all'interno dell'Ente).
Se l'Utente ha il sospetto che le proprie credenziali di autenticazione siano state identificate da qualcuno, o il sospetto di un utilizzo non autorizzato del proprio account e delle risorse a questo associate, lo stesso è tenuto a modificare immediatamente la password e/o a segnalare la violazione all'amministratore del sistema nonché al Responsabile privacy di riferimento.
Ogni Utente è responsabile dell'utilizzo del proprio account Utente.
In caso di assenza improvvisa o prolungata del lavoratore e per improrogabili necessità legate all'attività lavorativa, per le esigenze produttive aziendali o per la sicurezza ed operatività delle risorse informatiche dell'Ente, lo stesso si riserva la facoltà di accedere a qualsiasi dotazione e/o apparato assegnato in uso all'Utente per mezzo dell'intervento dell'Amministratore di sistema.
Si ricorda, infine, che i beni e la strumentazione informatica oggetto del presente disciplinare interno rimane di esclusivo dominio dell'Ente, il quale, in virtù dei rapporti instaurati con gli utenti, ne disciplina l'affidamento.

Gestione e utilizzo delle password
Dopo la prima comunicazione delle credenziali di autenticazione da parte dell'amministratore di sistema, l'Utente ha il compito di modificare, al suo primo utilizzo, la propria password, procedendo allo stesso modo ogni 6 mesi. In caso di trattamento di categorie particolari di dati, di cui agli artt. 9 e 10 del Regolamento UE 2016/679, la parola chiave è modificata ogni 3 mesi.
L'Utente, nel definire il valore della password, deve rispettare le seguenti regole:

- utilizzare almeno 8 caratteri alfanumerici, inclusi i caratteri speciali (#, %, etc.), di cui almeno uno numerico;
- la password deve contenere almeno un carattere maiuscolo, un carattere minuscolo, un numero o un carattere non alfanumerico tipo "@#§£$%...";
- evitare di includere parti del nome, cognome e/o comunque elementi a lui agevolmente riconducibili;
- evitare l'utilizzo di password comuni e/o prevedibili;
- proteggere con la massima cura la riservatezza della password ed utilizzarla entro i limiti di autorizzazione concessi.

Si ricorda che scrivere la password su post-it o altri supporti non è conforme alla normativa e costituisce violazione del presente disciplinare interno.

Cessazione degli Account
In caso di interruzione del rapporto di lavoro con l'Utente, le credenziali di autenticazione di cui sopra verranno disabilitate entro un periodo massimo di 30 giorni da quella data; entro 6 mesi, invece, si disporrà la definitiva e totale cancellazione dell'account Utente.

ART. 8
POSTAZIONI DI LAVORO

Per postazione di lavoro si intende il complesso unitario di Personal Computer (di seguito, PC), notebook, accessori, periferiche e ogni altro *devices* concesso, dall'Ente, in utilizzo all'Utente. L'assegnatario di tali beni e strumenti informatici aziendali, pertanto, ha il compito di farne un uso compatibile con i principi di diligenza sanciti nel codice civile.
Al fine di disciplinare un corretto utilizzo di tali beni, L'Ente ha adottato le regole tecniche, che di seguito si riportano:

- Ogni PC, notebook (accessori e periferiche incluse), e altro *devices*, sia esso acquistato, noleggiato, o affidato in locazione, rimane di esclusiva proprietà dell'Ente, ed è concesso all'Utente per lo svolgimento delle proprie mansioni lavorative e comunque per finalità strettamente attinenti l'attività svolta;
- È dovere di ogni Utente usare i computer e gli altri dispositivi a lui affidati responsabilmente e professionalmente;
- Il PC e gli altri dispositivi di cui sopra devono essere utilizzati con hardware e software autorizzati dall'Ente. Per utilizzare software o applicativi non presenti nella dotazione standard fornita, si necessita di espressa richiesta scritta dell'Utente indirizzata al proprio responsabile privacy di riferimento, il quale ne valuterà i requisiti tecnici e l'aderenza alle policy interne ed al ruolo ricoperto in azienda;
- Le postazioni di lavoro non devono essere lasciate incustodite con le sessioni utenti attive;
- Quando un Utente si allontana dalla propria postazione di lavoro, deve bloccare tastiera e schermo con un programma salvaschermo (screensaver) protetto da password o effettuare il log-out dalla sessione;
- L'Utente deve segnalare con la massima tempestività all'amministratore del sistema ovvero al proprio Responsabile di riferimento eventuali guasti tecnici, problematiche tecniche o il cattivo funzionamento delle apparecchiature;
- È fatto divieto di cedere in uso, anche temporaneo, le attrezzature e i beni informatici aziendali a soggetti terzi;
- L'Ente si riserva la facoltà di rimuovere qualsiasi elemento hardware e/o software la cui installazione non sia stata appositamente e preventivamente prevista o autorizzata.

Gli apparecchi di proprietà personale dell'Utente quali computer portatili, telefoni cellulari, agende palmari (PDA), hard disk esterni, penne USB, lettori musicali o di altro tipo, fotocamere digitali, ecc. non potranno essere collegati ai computer o alle reti informatiche aziendali, salvo preventiva autorizzazione scritta dell'Ente.

ART. 9
BACKUP DATI

Al fine di garantire la sicurezza dei dati aziendali, sono previste operazioni di backup dei dati, effettuate periodicamente, con cadenza settimanale. I Server di backup sono ubicati all'interno dell'ente in una stanza refrigerata e chiusa a chiave.
È unicamente designato a tale attività l'amministratore di sistema nominato, il quale effettuerà le copie di backup dei dispositivi in dotazione dell'Ente, su cui vengono registrati tutti i dati acquisiti, strettamente necessari per lo scopo perseguito.

CAPO III – CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI

ART. 10
PERSONAL COMPUTER E COMPUTER PORTATILI

Gli utenti utilizzano per l'espletamento delle proprie mansioni dispositivi di proprietà dell'Ente; ne consegue che gli stessi sono tenuti al rispetto delle seguenti regole:
- Non è consentito modificare la configurazione hardware e software del proprio PC, se non previa esplicita autorizzazione dell'Ente che la esegue per mezzo dell'amministratore del sistema
- Non è consentito rimuovere, danneggiare o asportare componenti hardware;

- Non è consentito installare autonomamente programmi informatici, software ed ogni altro applicativo non autorizzato espressamente dall'Ente;
- E' onere dell'Utente, in relazione alle sue competenze, eseguire richieste di aggiornamento sulla propria postazione di lavoro derivanti da software antivirus nonché sospendere ogni attività in caso di minacce *virus* o altri malfunzionamenti, segnalando prontamente l'accaduto all'amministratore del sistema;
- è onere dell'Utente spegnere il proprio PC o computer portatile al termine del lavoro.

Per quanto concerne, invece, la gestione dei computer portatili, l'Utente ha l'obbligo di custodirli con diligenza e in luogo protetto durante gli spostamenti, rimuovendo gli eventuali *files* elaborati prima della sua riconsegna.
Non è consentito all'Utente caricare o inserire all'interno del portatile qualsiasi dato personale non attinente con l'attività lavorativa svolta. In ogni caso, al fine di evitare e/o ridurre al minimo la possibile circolazione di dati personali sull'apparecchio, si ricorda agli utenti di cancellare tutti i dati eventualmente presenti prima di consegnare il portatile agli uffici competenti per la restituzione o la riparazione.

ART. 11
SOFTWARE

Premesso che l'installazione di software privi di regolare licenza non è consentita in nessun caso, gli utenti dovranno ottenere espressa autorizzazione dell'Ente per installare o comunque utilizzare qualsiasi programma o software dotato di licenza non proprietaria ("freeware" o "shareware").
L'Ente richiama l'attenzione del proprio personale su alcuni aspetti fondamentali che l'Utente è tenuto ad osservare per un corretto utilizzo del software in azienda:

- L'Ente acquista le licenze d'uso dei software da vari fornitori esterni. L'Utente, pertanto, è soggetto a limitazioni nell'utilizzo di tali programmi e della relativa documentazione e non ha il diritto di riprodurlo in deroga ai diritti concessigli. Tutti gli utenti sono quindi tenuti a utilizzare il software entro i limiti specificati nei contratti di licenza.
- Non è consentito fare né il download né l'upload tramite internet di software non autorizzato.
- L' Ente, sulla scorta di quanto disposto dalle normative a tutela della proprietà intellettuale e del diritto d'autore, ricorda che le persone coinvolte nella riproduzione illegale del software sono responsabili sia civilmente che penalmente e quindi possono essere condannate al pagamento dei danni e anche alla reclusione.
- L'Ente non tollererà la duplicazione illegale del software.

ART. 12
DISPOSITIVI DI MEMORIA PORTATILI

Per dispositivi di memoria portatili si intendono tutti quei dispositivi che consentono di copiare o archiviare dati, files, o documenti esternamente al computer. Sono considerati tali CD-ROM, DVD, penne o chiavi di memoria USB, riproduttori musicali MP3, fotocamere digitali, dischi rigidi esterni, etc.
L'utilizzo di tali supporti risponde alle direttive che di seguito si riportano:

- non è consentito utilizzare supporti rimovibili personali, se non preventivamente autorizzati per iscritto dall'Ente;
- è onere dell'Utente custodire i supporti magnetici contenenti dati sensibili e giudiziari in armadi chiusi a chiave, onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto;

- si precisa che, ove autorizzati in base a quanto sopra disposto, una volta connessi all'infrastruttura informatica dell'Ente, i dispositivi saranno soggetti (ove compatibili) al presene disciplinare interno.

ART. 13
STAMPANTI, FOTOCOPIATRICI, SCANNER E FAX

L'utilizzo dei suddetti strumenti deve avvenire sempre per scopi professionali. Non è consentito un utilizzo per fini diversi o privati, salvo una specifica autorizzazione da parte dell'Ente.
E' richiesta una particolare attenzione quando si invia su una stampante condivisa documenti aventi ad oggetto dati personali o informazioni riservate; ciò al fine di evitare che persone non autorizzate possano venirne a conoscenza. Si richiede quindi di evitare di lasciare le stampe incustodite e ritirarne immediatamente le copie non appena uscite dalla stampa.
L'utilizzo dei fax per l'invio di documenti che hanno natura strettamente confidenziale, è generalmente da evitare. Nei casi in cui questo sia necessario, si deve preventivamente avvisare il destinatario, in modo da ridurre il rischio che persone non autorizzate possano venirne a conoscenza, e successivamente chiedere la conferma telefonica di avvenuta ricezione.
L'utilizzo della funzione di scannerizzazione di documenti analogici in digitale, comporta l'immediato trasferimento del file dalla cartella di destinazione condivisa da ciascun PC all'inserimento delle apposite cartelle presenti su ciascuna postazione.

CAPO IV – GESTIONE DELLE COMUNICAZIONI TELEMATICHE

ART. 14
GESTIONE UTILIZZO DELLA RETE INTERNET

Ogni Utente potrà essere abilitato, dalla Ente, alla navigazione Internet. Col presente disciplinare interno si richiama gli utenti ad una particolare attenzione nell'utilizzo di Internet e dei servizi relativi, in quanto ogni operazione posta in essere è associata all'"Indirizzo Internet Pubblico" assegnato all'Ente stesso.
Internet è uno strumento messo a disposizione degli utenti per uso professionale. Ciascun lavoratore, pertanto, deve usare la rete Internet in maniera appropriata, tenendo presente che ogni sito web può essere governato da leggi diverse da quelle vigenti in Italia; l'Utente deve, quindi, prendere ogni precauzione a tale riguardo.

Le norme di comportamento da osservare nell'utilizzo delle connessioni ad Internet sono le seguenti:

a. L'utilizzo è consentito esclusivamente per scopi aziendali e, pertanto, non è consentito navigare in siti non attinenti allo svolgimento delle proprie mansioni lavorative.
b. Non è consentita l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi espressamente autorizzati dall'Ente.
c. È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
d. Non sono permesse, se non per motivi professionali, la partecipazione a forum, l'utilizzo di chat-line o di bacheche elettroniche e le registrazioni in *guest-book*, anche utilizzando pseudonimi (o nicknames).

e. Non è consentita la navigazione in siti e la memorizzazione di documenti informatici di natura oltraggiosa, pornografica, pedopornografica e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
f. È consentito l'utilizzo di soluzioni di Instant Messanger e/o chat esclusivamente per scopi professionali ed attraverso gli strumenti ed i software messi a disposizione dall'Ente.
g. Non è consentito l'utilizzo di sistemi di social networking sul luogo di lavoro o durante l'orario lavorativo.
h. Non è consentito lo scambio e/o la condivisione (es. i c.d. sistemi di Peer-to-Peer) a qualsiasi titolo, anche se non a scopo di lucro, di materiale audiovisivo, cinematografico, fotografico, informatico, etc., protetto da copyright.
i. Non è consentito sfruttare i marchi registrati, i segni distintivi e ogni altro bene immateriale di proprietà dell'Ente in una qualsiasi pagina web o pubblicandoli su Internet, a meno che tale azione non sia stata approvata espressamente;

Per facilitare il rispetto delle predette regole, l'Ente si riserva, per mezzo dell'amministratore di sistema, la facoltà di configurare specifici filtri che inibiscono l'accesso ai contenuti ivi non consentiti (con esclusione dei siti istituzionali) e che prevengono operazioni non correlate all'attività lavorativa (es. upload, restrizione nella navigazione, download di *file* o software).

ART. 15
SANZIONI

L'eventuale violazione di quanto previsto dal presente disciplinare interno – rilevante anche ai sensi degli art. 2104 e 2105 c.c. - potrà comportare l'applicazione di sanzioni disciplinari in base a quanto previsto dall'art. 7 dello Statuto dei Lavoratori.
L'Ente avrà cura di informare senza ritardo (e senza necessità di preventive contestazioni e/o addebiti formali) le autorità competenti, nel caso venga commesso un reato, o la cui commissione sia ritenuta probabile o solo sospettata, tramite l'utilizzo illecito o non conforme dei beni e degli strumenti informatici aziendali.
Si precisa, infine, che in caso di violazione accertata da parte degli utenti delle regole e degli obblighi esposti in questo disciplinare, L'Ente si riserva la facoltà di sospendere, bloccare o limitare gli accessi di un account, quando appare ragionevolmente necessario per proteggere l'integrità, la sicurezza e/o la funzionalità dei propri beni e strumenti informatici.

ART. 16
INFORMATIVA AGLI UTENTI EX ART. 13 Regolamento UE n. 2016/679

Il presente disciplinare interno, nella parte in cui contiene le regole per l'utilizzo dei beni e degli strumenti informatici aziendali, e relativamente ai trattamenti di dati personali svolti dall'Ente e finalizzati alla effettuazione di controlli leciti, così come definiti nell'art. 5, vale quale informativa ex. art. 13 del Regolamento UE n. 2016/679.

ART. 17
COMUNICAZIONI

Il presente disciplinare interno è messo a disposizione degli utenti, per la consultazione, al momento dell'assegnazione di un account Utente. Sulla intranet aziendale, ovvero presso la bacheca aziendale è pubblicata la versione più aggiornata dello stesso allo scopo di facilitarne la conoscibilità a tutti gli interessati.

Ad ogni aggiornamento del presente documento, ne sarà data comunicazione sulle bacheche aziendali e tramite l'invio di apposito messaggio e-mail. Tutti gli utenti sono tenuti a conformarsi alla versione più aggiornata del presente disciplinare.
Le autorizzazioni e/o concessioni richieste dal presente disciplinare ovvero poste nella facoltà degli utenti potranno essere comunicate all'Ente per mezzo di qualsiasi strumento che ne garantisca la tracciabilità (es: e-mail).

Il presente regolamento si compone di n. 11 pagine, compreso la presente.

L'Amministrazione