I REGOLAMENTI PROVINCIALI: N. 100

PROVINCIA DI PADOVA

REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI

Approvato con D.P. in data 6.7.2022 n. 79 di reg. e modificato con D.P. in data 28.8.2023 n. 118 di reg.

Sommario

1. Definizioni

Antivirus: programma che individua, previene e disattiva o rimuove programmi dannosi, come virus e worm.

Autorizzato: ogni Utente, come sotto identificato, che nell'ambito dell'attività assegnatagli, utilizza credenziali di accesso a strumenti informatici per il trattamento di dati.

Backup: copia di riserva di un disco, di una parte del disco o di uno o più file su supporti di memorizzazione diversi da quello in uso.

Chat: servizio offerto da Internet, che permette mediante apposito software una 'conversazione' fra più interlocutori costituita da uno scambio di messaggi scritti che appaiono in tempo reale sul monitor di ciascun partecipante.

Chiave USB: o unità flash USB o penna USB (anche in inglese USB flash drive, o pendrive) è una memoria di massa portatile di dimensioni molto contenute che si collega al computer mediante la porta USB.

CIE: Carta d'Identità Elettronica (La Carta di identità elettronica (CIE) | IPZS)

Client: Computer o programma collegato ad un altro (computer o programma) a cui inoltra le richieste dell'Utente.

Credenziali di autenticazione: sono le chiavi di accesso a strumenti informatici, procedure e dispositivi.

Dati: l'insieme di informazioni di cui un Utente, come sotto identificato, viene a conoscenza e di cui deve garantire la riservatezza e la segretezza.

Dati personali: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (art. 4 GDPR).

Dati particolari: dati personali che, per la loro delicatezza, richiedono particolari cautele; sono qui dati idonei a rilevare origine raziale o etnica, opinioni politiche, convinzioni religiose, appartenenza sindacale, dati biometrici, o dati relativi allo stato di salute.

Dipendente: personale dell'Ente assunto con qualsiasi tipo di forma contrattuale, anche in stage o tirocinio.

Download: è l'azione di ricevere o prelevare dalla rete informatica un file trasferendolo sul disco rigido del computer o su altra periferica dell'utente.

File: porzione di memoria (fissa o mobile) che contiene un insieme organizzato di informazioni omogenee.

File sharing: condivisione di file all'interno di una rete di calcolatori e tipicamente utilizza una delle seguenti architetture: client-server, peer-to-peer (rete informatica in cui i nodi sono gerarchizzati sotto forma di nodi equivalenti o paritari (in inglese peer) che possono cioè fungere sia da client che da server verso gli altri nodi della rete).

GDPR: General Data Protection Regulation - Regolamento Generale sulla Protezione dei Dati - Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016

Interessato: La persona fisica cui si riferiscono i dati personali.

LAN: è l'acronimo del termine inglese Local Area Network, in italiano "rete locale". Identifica una rete costituita da computer collegati tra loro, dalle interconnessioni e dalle periferiche condivise in un ambito fisico delimitato.

Malware: abbreviazione per malicious software (che significa letteralmente software malintenzionato, ma di solito tradotto come software dannoso), indica un qualsiasi programma

informatico usato per disturbare le operazioni svolte da un computer, rubare informazioni sensibili, accedere a sistemi informatici privati, o mostrare pubblicità indesiderata

Password: componente da mantenere riservata associata all'autenticazione di una persona e solo a questa nota.

Postazione di lavoro (PDL): luogo attrezzato per svolgere un'attività lavorativa dotato di personal computer (PC) o computer portatile ed eventuali altre unità hardware collegate alla rete dell'Ente inclusi tablet e smartphone.

Phishing: tipo di truffa effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione mail.

Ransomware: è un tipo di malware che limita l'accesso del dispositivo che infetta, richiedendo un riscatto (ransom in Inglese) da pagare per rimuovere la limitazione.

Repository: in un repository sono raccolti dati e informazioni in formato digitale, valorizzati e archiviati sulla base di metadati che ne permettono la rapida individuazione, anche grazie alla creazione di tabelle relazionali. Grazie alla sua peculiare architettura, un repository consente di gestire in modo ottimale anche grandi volumi di dati.

Rete locale: una Local Area Network (LAN) è una rete informatica di collegamento tra più computer, estendibile anche a dispositivi periferici condivisi, che copre un'area limitata, come un'abitazione, una scuola, un'azienda o un complesso di edifici adiacenti.

Server: computer denominato servente o programma a cui altri (computer o programmi) si collegano per l'elaborazione delle richieste dell'Utente.

SPID: Sistema Pubblico di Identità Digitale (SPID - Sistema Pubblico di identità Digitale)

Strumento (informatico/telematico): personal computer (PC) e altra unità hardware quale periferica/dispositivo elettronico, anche ad alta tecnologia e di piccole dimensioni (smartphone, e-book reader, tablet ecc.), risorse di rete, posta elettronica (e-mail) ed altri strumenti con relativi software e applicativi. Gli Strumenti, nonché le relative reti dell'Ente a cui è possibile accedere tramite gli stessi, sono domicilio informatico (art. 615-ter C.P.) dell'ente Provincia di Padova.

Trattamento: qualsiasi operazione compiuta con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la consultazione, l'adattamento, la modifica, la trasmissione, la diffusione, la cancellazione o distruzione.

Upload: è il processo di invio di un file (o più genericamente di un flusso finito di dati o informazioni) ad un sistema remoto attraverso una rete informatica.

Utente: È la persona (dipendente, collaboratore, consulente esterno, carica elettiva, volontario, altro operatore) autorizzata ad accedere mediante consegna di credenziali di autenticazione alla rete informatica dell'Ente, ad internet e alla posta elettronica, agli applicativi dell'Ente e alle altre risorse informatiche e telematiche dell'Ente. Nell'ambito dell'attività assegnata tratta dati (nell'accezione definita all'interno del presente documento) riferiti all'Ente.

Virus: programma appartenente alla categoria dei malware che, una volta eseguito, infetta dei file in modo da arrecare danni al sistema, rallentando o rendendo inutilizzabile il dispositivo infetto.

2. Scopo

2.1. Finalità del documento e contesto normativo

Prescrivere regole uniformi di utilizzo per tutti gli Utenti dell'Ente sugli Strumenti informatici e telematici e fornire le indicazioni necessarie con l'obiettivo principale di evitare il verificarsi di qualsiasi abuso o uso non conforme nel pieno rispetto delle normative vigenti.

Il contesto normativo fa riferimento in particolare a quanto disposto dal Regolamento UE 2016/679 (GDPR), dal D. Lgs. 196/2003 così come modificato dal D. Lgs. 101/2018 e da quanto disposto dalla Legge n. 300/1970 (c.d. Statuto dei Lavoratori) così come modificata dal D. Lgs. 14 settembre 2015, n. 151; il documento è stato inoltre redatto ai sensi di quanto disposto nei provvedimenti in tema dal Garante per la Protezione dei Dati Personali (si veda in particolare Provv. 1 marzo 2007- Linee Guida del Garante per posta elettronica e internet) e a quanto disposto dalla Direttiva n. 2/2009 del Dipartimento Funzione Pubblica avente ad oggetto "Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro".

3. Destinatari

3.1. Campo di applicazione

Il presente Regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'Ente a prescindere dalla tipologia di rapporto contrattuale con la stessa intrattenuto (a titolo esemplificativo lavoratori somministrati, collaboratori a progetto, in stage, collaboratori e professionisti esterni, amministratori, volontari e altro) oltre che ai dipendenti e collaboratori delle società esterne affidatarie di servizi, autorizzati ad accedere alla rete informatica dell'Ente o che si trovino ad operare con dati o Strumenti dell'Ente (tutti identificati nel presente documento col termine di "**Utenti"**).

Gli eventuali controlli disposti in conformità e nel rispetto della vigente normativa escludono finalità di monitoraggio diretto ed intenzionale dell'attività lavorativa.

La progressiva diffusione delle nuove tecnologie informatiche ed in particolare l'accesso alla rete internet dal computer espone l'Ente a possibili rischi di un coinvolgimento di rilevanza sia civile, sia penale, sia amministrativa, creando problemi alla sicurezza e all'immagine dell'Ente stesso.

Con il primo utilizzo degli Strumenti informatici e telematici dell'Ente l'Utente dichiara di aver attentamente letto ed espressamente accettato tutti i termini e le condizioni di utilizzo del servizio medesimo indicati nel presente Regolamento, al quale dovrà attenersi scrupolosamente.

Il mancato rispetto del Regolamento comporterà immediati provvedimenti che saranno valutati a seconda della gravità dell'azione intrapresa e della sua recidività.

3.2. Attori e responsabilità

A) Dirigente Sistemi Informativi
   - È responsabile della progettazione del sistema, delle reti e stabilisce i controlli;
   - verifica periodicamente l'attività degli Amministratori di Sistema attraverso audit interni;
   - è responsabile del governo del sistema informativo ovvero delle attività gestite dal management dei sistemi informativi al fine di trovare la migliore integrazione in ottica di riduzione dei rischi.

B) Dirigente competente / Segretario Direttore Generale
   - Verifica periodicamente l'attività attraverso audit interni;
   - autorizza gli accessi alla rete per l'utenza di competenza.

C) P.O. Sistemi Informativi
   - Segnala immediatamente al Dirigente eventuali situazioni di rischio della sicurezza dei sistemi

e della rete;

- vigila sugli Amministratori di Sistema e verifica con periodicità almeno annuale i profili e le autorizzazioni degli utenti Amministratori di Sistema.
- autorizza gli accessi alla rete per l'utenza di competenza.

D) Amministratori di Sistema

Personale sistemistico e di networking con accesso alle informazioni secondo le regole disposte dal Dirigente dei Sistemi Informativi che li nomina direttamente e formalmente. Le responsabilità sono definite in dettaglio successivamente nel presente documento.

E) Utente

È responsabile degli Strumenti informatici e telematici dell'Ente a lui assegnati e ha il dovere di segnalare tempestivamente situazioni di rischio per la sicurezza dei dati e della rete. È altresì responsabile della corretta custodia delle proprie password e degli account (dati identificativi) che gli consentono l'accesso ai servizi dell'Ente.

F) Fornitori di prodotti e servizi

Coloro che provvedono all'approvigionamento di beni e/o servizi all'Ente. Il Titolare del trattamento in fase di aggiudicazione nomina il Responsabile del trattamento nell'ambito del contratto, il quale è tenuto ad accettare le regole presenti nel presente documento.

3.3. Responsabilità dell'Utente

I dispositivi assegnati sono uno strumento lavorativo nella disponibilità dell'Utente esclusivamente per un fine di carattere lavorativo. Gli Strumenti, quindi, non devono essere utilizzati per finalità private e diverse da quelle istituzionali.

L'Ente pertanto non potrà in ogni caso essere ritenuto responsabile per la perdita di contenuti a carattere non lavorativo (quali ad es. e-mail private, foto, documenti privati e/o d'identità, file musicali, filmati ecc.). Se durante le attività manutentive o di assistenza, dovessero essere rilevati i contenuti sopra citati, sarà facoltà del servizio sistemi informativi la cancellazione degli stessi.

Ogni Utente è personalmente responsabile del corretto utilizzo dei beni e delle risorse informatiche affidatigli nonché dei relativi dati trattati per finalità istituzionali.

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 dell'Ente stesso 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 istituzionali.

Ogni Utente, pertanto, è tenuto, in relazione al proprio ruolo e alle mansioni in concreto svolte, ad operare a tutela della sicurezza informatica dell'Ente, riportando al proprio Dirigente responsabile e al Dirigente del Servizio Sistemi Informativi senza ritardo eventuali rischi di cui è a conoscenza ovvero violazioni del presente documento.

Sono vietati comportamenti che dall'utilizzo degli Strumenti informatici possano creare un danno patrimoniale e/o di immagine all'Ente.

È vietato accedere ai siti internet mediante azioni inibenti dei filtri, sabotando o comunque superando o tentando di superare o disabilitando i sistemi adottati dall'Ente per bloccare accessi non conformi. In ogni caso è vietato utilizzare software o altri strumenti che consentano la navigazione anonima o di bypassare tali filtri.

L'Utente assegnatario della PDL è responsabile del suo corretto utilizzo nel rispetto delle seguenti regole comportamentali:

- La PDL non deve essere accessibile a soggetti non autorizzati;

- la PDL è assegnata all'utente per lo svolgimento dell'attività lavorativa ed è consentito l'uso ad altri utenti autorizzati ognuno con propria identificazione personale da tenere strettamente riservata;
- l'utente non deve apportare modifiche alle configurazioni delle PDL che non siano state preventivamente autorizzate dal Servizio Sistemi Informativi;
- il personale ha l'obbligo si salvare il materiale relativo alla propria attività lavorativa solo sugli spazi di condivisione di rete messi a disposizione dall'Ente;
- durante l'allontanamento dalla PDL, l'utente deve bloccare la propria postazione per consentirne l'accesso solo tramite password;
- al termine della giornata lavorativa deve essere effettuato lo spegnimento della PDL.

È espressamente vietato:

1. Introdursi abusivamente nei sistemi informatici dell'Ente;
2. installare e utilizzare programmi che non siano stati regolarmente acquistati e/o utilizzati in modalità portable;
3. distruggere, deteriorare o rendere inservibili dati e/o strumenti informatici;
4. conservare documenti, foto o video non pertinenti l'attività lavorativa a contenuto osceno, violento, offensivo alla morale o alla pubblica decenza.

All'Utente è vietato l'utilizzo e il collegamento a dispositivi provinciali di memorie esterne personali (quali chiavi USB, memory card, cd-rom, DVD, macchine fotografiche, videocamere, tablet, ...).

Agli Utenti non è permesso svolgere la loro attività lavorativa con strumentazione personale (PC fissi, portatili, tablet, smartphone) connessi o meno alla rete informatica della Provincia di Padova se non espressamente autorizzati per iscritto dal Dirigente responsabile del servizio interessato sentito il Dirigente dei Sistemi Informativi.

In particolare, gli Utenti non dipendenti (ovvero i consulenti, collaboratori esterni e fornitori), possono utilizzare i propri Strumenti personali per memorizzare dati e informazioni inerenti l'attività dell'Ente solo se espressamente autorizzati per iscritto dal Dirigente responsabile del servizio interessato sentito il Dirigente dei Sistemi Informativi.

3.4. Compiti degli Amministratori di Sistema

L'Ente conferisce agli Amministratori di Sistema (secondo il Provvedimento generale del 27 novembre 2008 del Garante per la protezione dei dati personali) il compito di sovrintendere i beni e le risorse informatiche.

L'Amministratore di Sistema è una figura tecnica informatica interna (normalmente personale tecnico del Servizio Sistemi Informativi dell'Ente) o esterna a cui spetta il compito principale di mettere in atto misure tecniche per garantire un livello di sicurezza adeguato al rischio (art. 32 del Regolamento UE 2016/679 GDPR).

È altresì compito dell'Amministratore di Sistema:

1. Gestire l'hardware e il software di tutta la strumentazione informatica di appartenenza della Società;
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. verificare con periodicità almeno annuale i profili e le autorizzazioni degli utenti con accesso alla rete;
4. 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;
5. 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

6. rimuovere software, componenti hardware e dati contenuti di carattere non lavorativo, dalle risorse informatiche assegnate agli utenti, tali attività rientrano nelle normali attività di manutenzione, gestione della sicurezza, e della protezione dei dati;
7. provvedere alla sicurezza informatica dei sistemi informativi dell'Ente, nel rispetto di quanto prescritto dal Regolamento UE 2016/679 e successiva regolamentazione D. Lgs. 101/2018;
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 nel rispetto della normativa vigente.

In ogni caso l'Amministratore di sistema non deve e non può svolgere i propri compiti in funzione di controllo a distanza dell'attività dei lavoratori o di indagine sugli stessi, fatta salva eventuale specifica richiesta dell'Autorità giudiziaria.

4. Credenziali

4.1. Le credenziali di autenticazione

Le credenziali di autenticazione per l'accesso alla rete, ai PC ed alle applicazioni, vengono creati dagli Amministratori di Sistema, previa formale richiesta del Dirigente del Servizio, o P.O. sua delegata, nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente.

Il Settore Risorse Umane è tenuto a comunicare al Servizio Sistemi Informativi l'attivazione e la cessazione del rapporto di lavoro, nonché l'eventuale trasferimento ad altro servizio e/o mansione del dipendente/utente. La comunicazione può avvenire anche con modalità automatiche.

Le richieste delle credenziali vengono inoltrate attraverso l'apposito sistema informatico di Help Desk di assistenza del portale Intranet provinciale, o in forma scritta.

Le credenziali di autenticazione vengono disattivate dopo 3 mesi di disuso, eccetto quelle preventivamente autorizzate per scopi di gestione tecnica.

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (nome utente) assegnato dal Servizio Sistemi Informativi, associato ad una parola chiave (password) riservata, che dovrà essere custodita dall'Utente con la massima diligenza e non divulgata o comunicata a terzi. In tal senso costituiscono lo strumento di associazione dell'utente con le operazioni svolte. In particolare il nome utente e la password costituiscono una firma elettronica che, in assenza di denuncia di smarrimento o richiesta di blocco, fanno presumere che le attività svolte con tale utenza siano riconducibili all'assegnatario e costituiscono pertanto un'identità digitale.

4.2. Login e Logout

Il "Login" è l'operazione con la quale l'Utente si autentica all'interno della propria PDL e si connette al sistema informatico provinciale o ad una parte di esso, dichiarando il proprio nome utente e password, aprendo una sessione di lavoro. In molti casi è necessario effettuare più login, tanti quanti sono gli ambienti di lavoro (ad es. applicativi web, intranet), ognuno dei quali richiede un username e una password.

Il "Logout" è l'operazione con cui viene chiusa la sessione di lavoro. Al termine dell'attività, tutte le applicazioni devono essere chiuse secondo le regole previste dall'applicazione stessa.

4.3. Le password

Le password quale metodo di autenticazione assegnato dall'Ente, hanno lo scopo di garantire l'accesso protetto ad uno strumento hardware oppure ad un applicativo software.

La prima caratteristica di una password è la segretezza, e cioè il fatto che non venga svelata ad altri soggetti. La divulgazione delle proprie password o la trascuratezza nella loro conservazione possono causare gravi danni al proprio lavoro, a quello dei colleghi e dell'Ente nel suo complesso, pertanto, le password dovranno essere custodite dall'Utente con la massima diligenza e non divulgate.

Nel tempo anche la password più sicura perde la sua segretezza. Per questo motivo è buona norma cambiarle con una certa frequenza e comunque ogni qualvolta si ritiene che la stessa abbia perso la caratteristica di segretezza.

L'Ente ha implementato alcuni meccanismi che permettono di aiutare e supportare gli utenti autorizzati in una corretta gestione delle password definendo, laddove tecnicamente possibile, una lunghezza minima delle password, la loro complessità e le politiche di cambiamento delle stesse in funzione di quanto richiesto dalle normative vigenti.

La password, formata da lettere maiuscole e minuscole, numeri e caratteri speciali, in combinazione fra loro, deve essere composta da almeno dodici caratteri e non deve contenere riferimenti agevolmente riconducibili all'Utente.

È vietato trascrivere o memorizzare la password su supporti intercettabili da altre persone.

Le password e/o PIN sono assolutamente personali e non vanno mai comunicate ad altri. Non vanno inoltre utilizzate le credenziali di altri colleghi.

Le password temporanee devono essere obbligatoriamente cambiate al primo nuovo accesso.

Occorre sostituire immediatamente una password non appena si abbia il dubbio che sia diventata poco "sicura" indipendentemente dalla data dell'ultimo cambio.

È vietato digitare la propria password in presenza di altri soggetti che possano vedere la tastiera, anche se collaboratori o dipendenti dell'Ente.

In qualsiasi momento, per motivi tecnici o di sicurezza, l'Ente si riserva il diritto di revocare all'Utente il permesso di accedere ad un sistema hardware o software a cui era precedentemente autorizzato, rimuovendo il nome utente o modificando/cancellando la password ad esso associata.

In particolare la password relativa ad un sistema può essere reimpostata dagli Amministratori di Sistema per le seguenti esigenze:

- Richiesta dell'utente per smarrimento della password;
- richiesta di accesso al sistema con il profilo dell'utente per risoluzione di problematiche di carattere tecnico (es: malfunzionamento del software);
- rischio imminente di compromissione dei dati per attacco informatico;
- richiesta dell'autorità giudiziaria;
- interventi urgenti a protezione della rete provinciale e del funzionamento dei sistemi.

Al fine di una corretta gestione delle password, l'Ente stabilisce il divieto di utilizzare come propria password:

- Nome e/o cognome e loro parti;
- lo username assegnato;
- un indirizzo di posta elettronica (e-mail);
- parole comuni (in Inglese e in Italiano);
- date, mesi dell'anno e giorni della settimana, anche in lingua straniera;
- parole banali e/o di facile intuizione, ad es. pippo, password e palindromi (simmetria: radar);
- ripetizioni di sequenze di caratteri o numeri (es. abcabcabc 123456);
- password già impiegate in precedenza.

4.4. Esclusione all'uso degli strumenti informatici

Nell'affidamento di mansioni o incarichi nel rapporto lavorativo o di consulenza, l'Ente valuta la presenza dei presupposti per l'autorizzazione all'uso dei vari Strumenti informatici, dell'accesso ad internet, della posta elettronica e più in generale di tutti i servizi informatici e di telecomunicazioni da parte degli Utenti.

Al venir meno delle esigenze per l'utilizzo degli Strumenti informatici, delle applicazioni, di internet e della posta elettronica, l'Ente provvede a revocare l'autorizzazione.

È fatto esplicito divieto agli Utenti di far accedere persone non autorizzate agli Strumenti informatici dell'Ente.

5. Postazioni di lavoro (PDL)

Per postazione di lavoro (PDL) si intende il complesso unitario di Personal Computer (di seguito, PC), notebook/portatile, accessori, periferiche e ogni altro dispositivo concesso, dall'Ente, in utilizzo all'Utente compresi gli applicativi (software). L'assegnatario di tali beni e strumenti informatici, pertanto, ha il compito di farne un uso compatibile con i principi di diligenza sanciti nel codice civile e conformi in linea con le attività lavorative svolte. L'Utente dovrà altresì eseguire le operazioni descritte nel presente documento, a protezione della propria PDL, nel rispetto della sicurezza e dell'integrità del patrimonio informativo dell'Ente.

5.1. Obblighi

L'utilizzo dei dispositivi assegnati e la gestione dei dati ivi contenuti devono svolgersi nel rispetto della sicurezza e dell'integrità del patrimonio informativo.

L' Utente deve eseguire le operazioni seguenti:

1. Bloccare la propria PDL prima delle pause e, in generale, ogni qualvolta abbia bisogno di allontanarsi dalla propria postazione o in caso di prolungato inutilizzo dello stesso, preferibilmente impostando il logout automatico del Sistema Operativo;
2. chiudere la sessione (Logout) alla fine del proprio turno di lavoro;
3. spegnere lo Strumento dopo il Logout;
4. controllare sempre che non vi siano persone non autorizzate che possano prendere visione delle schermate dello Strumento (soprattutto all'atto dell'inserimento delle password).

Le politiche di sicurezza informatiche prevedono comunque, dove possibile, la disattivazione automatica della sessione (blocco dello Strumento) dopo un determinato intervallo di inattività.

5.2. Modalità d'uso delle PDL dell'Ente

Il sistema informatico è composto da un insieme di unità server centrali e macchine client connesse o meno ad una rete provinciale, comunque messe a disposizione dall'Ente agli Utenti per lo svolgimento dei compiti affidati e che utilizzano diversi sistemi operativi e applicativi.

L'Ente non effettua il backup dei dati memorizzati in locale sulle PDL dell'Utente pertanto tutti i dischi o altre unità di memorizzazione locali (es. disco C: interno al computer) non sono soggette a salvataggio da parte del personale incaricato dell'assistenza tecnica del Servizio Sistemi Informativi.

Qualsiasi file estraneo all'attività lavorativa o non espressamente autorizzato, non può, nemmeno in via transitoria, essere salvato nel personal computer o in rete.

I file creati, elaborati o modificati sulla PDL assegnata e di cui risulta necessario assicurare l'integrità dei dati in caso di rottura della PDL stessa, devono essere salvati nelle cartelle di rete dell'ufficio messe a disposizione dall'Ente.

Le cartelle utenti presenti nei server dell'Ente sono aree di condivisione di informazioni strettamente lavorative 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. Tutti i documenti per cui si renda necessaria la garanzia della conservazione devono essere posizioni sulle cartelle di rete o copiati sulle stesse periodicamente.

Il personale tecnico del Servizio Sistemi Informativi può in qualunque momento:

- Procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza sia sui personal computer/notebook degli Utenti sia sulle unità di rete;
- rimuovere qualsiasi elemento hardware la cui installazione non sia stata appositamente e preventivamente prevista o autorizzata.

Risulta opportuno che, con regolare periodicità (almeno ogni mese), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante in ossequio al principio della minimizzazione del trattamento dei dati.

5.3. Distruzione degli Strumenti

Ogni Strumento ed ogni memoria esterna affidati agli Utenti, (computer, notebook, tablet, smartphone, memory card, chiavi usb, hard disk, dvd, cd-rom, ecc.), al termine del loro utilizzo dovranno essere restituiti al Servizio Sistemi Informativi che provvederà a distruggerli o a ricondizionarli seguendo le norme di legge in vigore al momento. In particolare l'Ente provvederà a cancellare o a rendere inintelligibili i dati negli stessi memorizzati.

L'Ente e gli Amministratori di Sistema non possono essere ritenuti responsabili per la perdita di dati appartenenti all'Utente e non relativi all'ambito lavorativo contenuti in strumenti informatici provinciali.

5.4. Restituzione degli Strumenti

A seguito di una cessazione del rapporto lavorativo o di consulenza dell'Utente con l'Ente o, comunque, al venir meno, ad insindacabile giudizio dell'Ente, della permanenza dei presupposti per l'utilizzo degli Strumenti informatici, gli Utenti hanno i seguenti obblighi:

1. Procedere immediatamente alla restituzione degli Strumenti in uso al Servizio Sistemi Informativi;
2. divieto assoluto di formattare o alterare o manomettere o distruggere gli Strumenti assegnati o rendere inintelligibili i dati in essi contenuti tramite qualsiasi processo;
3. trasmettere all'ufficio competente dati di interesse per il proseguo delle attività istituzionali a cui era assegnato.

Le stesse regole si applicano anche in caso di restituzione dello Strumento in seguito a richiesta di manutenzione per guasto dello Strumento o in caso di controlli che l'Ente è tenuta ad effettuare sullo Strumento stesso.

5.5. Gestione dati delle PDL

In caso di interruzione del rapporto di lavoro con l'Utente, l'account utente verrà disabilitato alla data di cessazione.

Entro 30 giorni dalla data di cessazione del rapporto di lavoro si disporrà la definitiva e totale cancellazione dei dati contenuti nella PDL.

In caso di sostituzione della PDL, i dati di backup della PDL sostituita, saranno mantenuti in luogo sicuro e non accessibili se non agli Amministratori di Sistema preposti, per un tempo massimo di 30 giorni.

6. Utilizzo del computer dell'Ente

Il dispositivo consegnato all'Utente è uno strumento di lavoro e contiene tutti i software necessari a svolgere le attività affidate. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, rallentamenti del sistema, costi di manutenzione e, soprattutto, minacce alla sicurezza, ed è pertanto non consentito.

L'accesso all'elaboratore è protetto da password che deve essere custodita dall'Utente con la massima diligenza e non divulgata. Previa comunicazione all'Utente assegnatario, gli addetti all'assistenza tecnica informatica, potranno accedere ai computer, anche in remoto per attività di manutenzione ed assistenza.

In particolare l'Utente deve adottare le seguenti misure:

1. Utilizzare solo ed esclusivamente le aree di archiviazione dati messe a disposizione dall'Ente, senza pertanto creare altri file fuori di esse. Non è pertanto consentito utilizzare aree di scambio per inviare/ricevere file che non siano state autorizzate dal Servizio Sistemi Informativi e che non siano protette in lettura/scrittura da opportune credenziali di accesso;
2. in caso di allontanamento anche temporaneo dalla PDL (personal computer fisso o portatile) l'Utente deve bloccare lo schermo. L'Utente non deve lasciare la PDL accesa con il sistema operativo aperto e la propria password inserita. Al fine di evitare che persone non autorizzate effettuino accessi non permessi, l'utente deve attivare il salvaschermo con password o deve bloccare il computer (utilizzando la combinazione di tasti WIN+L);
3. spegnere il computer, o curarsi di effettuare il Logout in caso di assenze prolungate;
4. mantenere sul computer esclusivamente i dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, chiavette USB), assegnati dall'Ente;
5. non dare accesso al proprio computer ad altri Utenti, a meno che siano Utenti autorizzati con cui si condivide l'utilizzo della stessa PDL o a meno di necessità stringenti e comunque in questo caso sotto il proprio costante controllo.

All'Utente inoltre non è consentito:

1. Cedere in uso, anche temporaneo, le attrezzature e i beni informatici assegnati dall'Ente a soggetti terzi;
2. la gestione, la memorizzazione (anche temporanea) o il trattamento di file, documenti e/o informazioni personali o comunque non afferenti alle attività lavorative in nessun strumento informatico provinciale;
3. modificare le configurazioni già impostate sul personal computer;
4. utilizzare e/o installare programmi e/o sistemi senza la preventiva autorizzazione del Servizio Sistemi Informativi;
5. installare alcun software, né alcuna versione diversa, anche più recente, rispetto alle applicazioni o al sistema operativo presenti sul personal computer consegnato. Né è, peraltro, consentito fare copia del software installato al fine di farne un uso personale;
6. caricare sui dispositivi di memorizzazione messi a disposizione dall'Ente alcun documento, gioco, file musicale o audiovisivo o immagine diversi da quelli necessari allo svolgimento delle mansioni affidate;
7. aggiungere o collegare dispositivi hardware (ad esempio hard disk, driver, ecc.) o periferiche (telecamere, macchine fotografiche, smartphone, casse audio, chiavi USB ecc.) diversi da quelli consegnati, senza l'autorizzazione espressa dell'Ente;
8. creare o diffondere, intenzionalmente o per negligenza, programmi idonei a danneggiare il sistema informatico dell'Ente, quali per esempio virus, malware, trojan horses ecc.;
9. accedere, rivelare o utilizzare informazioni per le quali non si è autorizzati o comunque non necessarie per le mansioni svolte;
10. effettuare in proprio attività manutentive;
11. permettere attività manutentive da parte dei soggetti non espressamente autorizzati dal Servizio Sistemi Informativi dell'Ente.
12. utilizzare dispositivi di memorizzazione messi a disposizione dell'Ente su Strumenti non

provinciali.

6.1. Antivirus

I virus possono essere trasmessi tramite scambio di file via internet, via mail, scambio di supporti removibili, filesharing, chat ecc.

L'Ente impone su tutte le postazioni di lavoro l'utilizzo di un sistema antivirus correttamente installato, attivato continuamente e aggiornato automaticamente con frequenza almeno quotidiana.

L' Utente, da parte sua, deve rispettare le regole seguenti:

1. È vietato disattivare l'antivirus senza l'autorizzazione espressa del Servizio Sistemi Informativi;
2. porre massima attenzione all'email di dubbia provenienza evitando di aprirne gli allegati e segnalarle tempestivamente all'assistenza tecnica del Servizio Sistemi Informativi;
3. non utilizzare chiavette USB personali sui personal computer provinciali in quanto possono essere veicolo di virus che vengono così introdotti nella rete informatica dell'Ente.

È necessario contattare l'assistenza tecnica del Servizio Sistemi Informativi prima di procedere a qualsiasi attività potenzialmente in conflitto con quanto sopra ed anche qualora si sospetti che il computer/portatile assegnato risulti infettato da un virus informatico (ad esempio perché presenta un comportamento anomalo).

7. Utilizzo del computer dell'Ente in smart working / lavoro agile

Al fine di rendere possibile lo svolgimento della prestazione lavorativa il dipendente, potrà essere dotato dall'Amministrazione di un personal computer portatile e un cellulare, da utilizzarsi nel totale rispetto delle regole determinate dalla regolamentazione e in conformità con le indicazioni che gli saranno fornite.

In caso di Lavoro Agile, la dotazione soprariportata costituisce l'unica dotazione assegnata ed è quindi esclusa l'assegnazione di una postazione informatica fissa nella sede di lavoro.

Gli strumenti di lavoro affidati all'utente devono essere usati esclusivamente per lo svolgimento dell'attività lavorativa, nel rispetto di quanto previsto dai regolamenti dell'Amministrazione, e non per scopi personali o non connessi all'attività lavorativa.

L'utente ha l'obbligo di utilizzare e custodire gli strumenti di lavoro affidatigli con la massima cura e diligenza; un utilizzo scorretto degli strumenti messi a disposizione costituisce motivo di inadempimento di valenza Regolamento. In caso di guasto delle attrezzature in dotazione il lavoratore dovrà dare immediato avviso al proprio responsabile, all'assistenza informatica e dovrà consegnare lo strumento guastato non appena possibile.

Il dipendente che effettua attività di Smart-Working/Lavoro Agile può collegare il portatile messo a disposizione dall'Ente alla propria rete WI-FI per finalità istituzionali connesse alle attività lavorative svolte e nel rispetto del presente documento.

Per l'accesso alla rete dell'Ente normalmente viene utilizzato un programma installato sul portatile (VPN), che garantendo un accesso sicuro ai sistemi informatici dell'Ente, permette all'utente di svolgere l'attività lavorativa in modalità analoga a quella dell'ufficio.

Indipendentemente dalla modalità di lavoro, l'utente deve riportare in sede l'apparecchiatura, o effettuare periodicamente connessioni attraverso la VPN per permettere l'installazione di aggiornamenti del sistema, di programmi e lo scarico delle policy (regole) di sicurezza.

L'uso di strumentazione propria dovrà essere autorizzato dal personale preposto del Servizio Sistemi Informativi, che ne valuterà la compatibilità con i sistemi utilizzati dall'Ente e verificherà che questa disponga dei requisiti di sicurezza necessari e comunque su tali dispositivi non dovranno essere mai memorizzati dati dell'Ente (es. su dischi fissi, penne USB, ecc.).

In caso di utilizzo autorizzato di sistemi di proprietà dell'Utente, verrà fornita assistenza solo sulle componenti software che saranno fornite dall'Ente.

Nel caso in cui ci sia necessità di connettersi a rete wireless diverse da quella della propria abitazione si raccomanda, al fine di prevenire l'esposizione a cyber attacchi, di evitare il collegamento a reti sulle quali non si siano presenti adeguati sistemi di protezione e sicurezza.

8. Utilizzo del notebook

I computer portatili possono venire concessi in uso dall'Ente agli Utenti che durante gli spostamenti necessitino di disporre di archivi elettronici, supporti di automazione e/o di connessione alla rete dell'Ente.

Tali PDL portatili sono maggiormente esposte a rischi di sicurezza e danneggiamenti, furti e violazione delle informazioni contenute. Devono essere quindi verificate periodicamente dal Servizio Sistemi Informativi per l'installazione di aggiornamenti e/o patch di sicurezza. Tale attività avverrà su appuntamento concordato con il servizio Sistemi Informativi,

L'Ente, per tramite del Servizio Sistemi Informativi, non effettua il backup dei dati memorizzati in locale su tali dispositivi portatili.

Ai dispositivi portatili si applicano le regole di utilizzo previste per le PDL connesse in rete e comunque tutte le policy di sicurezza previste dall'Ente.

9. Utilizzo dello smartphone/tablet

Gli smartphone/tablet vengono forniti in dotazione dalla Provincia di Padova al proprio personale dipendente per motivi di servizio, su richiesta scritta del Dirigente competente o P.O. sua delegata.

L'utilizzo di apparecchi telefonici cellulari da parte di dipendenti risponde alla finalità di facilitare i contatti nel corso dello svolgimento dell'attività lavorativa ed a consentire comunicazioni urgenti o di emergenza.

L'Utente è responsabile dei dispositivi mobili assegnatigli dall'Ente e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro, non lasciarlo incustodito.

L'Ente, per tramite del Servizio Sistemi Informativi, non effettua il backup dei dati memorizzati in locale sui dispositivi mobili.

Il cellulare/smartphone provinciale affidato all'Utente è uno strumento di lavoro, ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa.

L'uso promiscuo del numero di telefono cellulare provinciale è consentito previa digitazione del prefisso per l'addebito delle chiamate personali. La ricezione o l'effettuazione di telefonate personali, senza tale prefisso, è consentita solo nel caso di comprovata necessità ed urgenza.

L'utilizzo del traffico voce e dati per finalità non istituzionali è consentito esclusivamente tramite l'attivazione del cosiddetto "Dual Billing". I costi derivanti dall'uso per fini privati saranno quindi addebitati direttamente dal concessionario all'affidatario dell'utenza. Sui cellulari forniti di carta SIM saranno inoltre impostate una o più "soglie di traffico", superate le quali l'utente sarà avvisato tramite SMS ed il Settore Sistemi Informativi tramite una e-mail informativa.

Qualora ve ne sia l'esigenza e previa richiesta dell'interessato, sarà favorita la portabilità del numero a privato e/o la cessione del dispositivo con relativo addebito, se previsto dalla convenzione in essere, in occasione dell'interruzione della collaborazione professionale con l'Ente.

L'apparato telefonico mobile e la SIM assegnati sono di uso esclusivo dell'Utente, non possono essere ceduti a terzi a nessun titolo e dovrà essere utilizzato solo per finalità istituzionali. In caso di uso collettivo del cellulare, la responsabilità è demandata al Responsabile dell'U.O./Servizio assegnatario.

È obbligatorio l'uso del PIN di sicurezza della SIM e del dispositivo di almeno 4 caratteri.

In caso di malfunzionamento del cellulare o della relativa scheda SIM o dei relativi accessori, l'Utente dovrà consegnare l'apparecchiatura completa al personale preposto dei Sistemi Informativi, il quale provvederà alle verifiche di competenza e alla eventuale sostituzione del cellulare, nei tempi e nelle modalità stabilite.

In caso di smarrimento o furto del cellulare e/o dei relativi accessori e/o della scheda SIM l'Utente è tenuto a sporgere immediata e formale denuncia alle autorità competenti e a darne tempestiva comunicazione scritta a telefoniamobile@provincia.padova.it ai fini dell'immediato blocco dell'utenza.

Nella comunicazione dovrà essere indicato in particolare, oltre al numero telefonico, il numero della SIM provinciale (ICCD) e il numero abbinato al telefono cellulare o CODICE IMEI al fine di consentire l'operazione di blocco immediato della scheda SIM e/o del cellulare.

All'atto di cessazione del rapporto di collaborazione con l'Ente, compresi i comandi verso altri enti, l'Utente affidatario del dispositivo dovrà riconsegnarlo personalmente all'ufficio della telefonia mobile presso il Servizio Sistemi Informativi.

Non è a carico del personale del Servizio Sistemi Informativi la responsabilità del salvataggio dei dati in esso contenuti in occasione della sostituzione/restituzione del dispositivo (es.

rubriche, foto, documenti, ecc.). L'Utente in ogni caso non potrà ricorrere contro l'Ente o terzi per la perdita di dati in esso contenuti.

La restituzione del dispositivo dovrà essere effettuata dall'Utente al personale preposto del Servizio Sistemi Informativi, che provvederà al ritiro, alla cancellazione dei dati.

Agli Utenti non è permesso configurare l'accesso alla posta elettronica su dispositivi non di proprietà dell'Ente.

I dispositivi mobile potranno essere gestiti tramite software di gestione remota dall'Ente ed in questo caso gli Utenti saranno registrati e i dispositivi controllati centralmente dal sistema in dotazione per la gestione e il mantenimento dei dispositivi stessi.

È responsabilità dell'Utente assegnatario del dispositivo mobile l'applicazione degli aggiornamenti periodici del sistema operativo e delle App presenti. In particolare degli aggiornamenti di sicurezza che dovranno essere controllati con cadenza settimanale e applicati al dispositivo.

L'Utente potrà installare soltanto applicazioni provenienti dai repository ufficiali dei fornitori dei dispositivi mobili (es. Google Play, Apple Store) per le esigenze di lavoro.

9.1. Principi di assegnazione

Ai fini del contenimento delle spese di funzionamento delle proprie strutture, l'Amministrazione adotta misure dirette a circoscrivere l'assegnazione di apparecchiature di telefonia mobile ai soli casi in cui il dipendente debba assicurare, per esigenze di servizio, pronta e costante reperibilità e limitatamente al periodo necessario allo svolgimento delle particolari attività che ne richiedono l'uso. Ciò premesso, il presente documento stabilisce che il personale dipendente può essere dotato di telefono cellulare esclusivamente per i seguenti casi:

- Esigenze connesse al servizio di pronta reperibilità;
- esigenze di immediata reperibilità di Dirigenti al fine di garantire il tempestivo intervento decisionale e le disposizioni operative;
- esigenze di immediata reperibilità di Dirigenti o di dipendenti del comparto, di tutti i ruoli, con compiti specifici professionali, caratterizzati dalla necessità di rapido intervento per attività urgenti ed indifferibili, nonché la continuità di erogazione dei servizi, ed attività che necessitino di comunicazioni che non possono essere altrimenti soddisfatte con impianti di telefonia fissa e/o altri strumenti di comunicazione quali la posta elettronica o maggiori costi rispetto all'uso del telefono cellulare;
- frequenti spostamenti tra plessi (reparti, servizi, uffici).

Ove possibile, in relazione alle esigenze da assolvere, deve privilegiarsi l'assegnazione di utenze e apparati di telefonia mobile standard. L'assegnazione può essere permanente o limitata per specifiche esigenze a determinati intervalli di tempo.

Gli apparecchi telefonici cellulari/smartphone di proprietà dell'Ente possono essere assegnati in dotazione ai dipendenti provinciali esclusivamente per motivi di servizio previa formale richiesta del Dirigente del Servizio o P.O. sua delegata.

Le richieste vengono inoltrate in forma scritta.

9.2. Controlli sull'utilizzo degli apparecchi

Il Servizio Sistemi Informativi su richiesta del Dirigente competente, fornisce i dettagli di traffico delle utenze assegnate al personale dipendente dei servizi coordinati.

9.3. Responsabilità

L'utilizzo dell'apparecchio in difformità da quanto prescritto nel presente documento può comportare a carico dell'assegnatario, oltre alla revoca immediata dell'assegnazione, ogni responsabilità giuridica, ivi comprese quella disciplinare e quella per risarcimento danni.

10. Utilizzo fax e telefoni fissi

Il telefono fisso assegnato all'utente è uno strumento di lavoro e ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa; non sono quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa. L'effettuazione di telefonate personali non è consentita.

È vietato l'utilizzo dei fax per fini personali sia per spedire sia per ricevere documentazione. Per finalità istituzionali si invita a prediligere forme di trasmissione alternative al fax.

11. Utilizzo stampanti e fotocopiatrici

È vietato l'utilizzo di scanner, fotocopiatrici, stampanti per fini personali.

Le stampanti di rete condivise sono installate per gruppi di lavoro, tramite policy di dominio.

Per quanto concerne l'uso delle stampanti gli utenti sono tenuti a:

1. Effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi;
2. prediligere le stampanti di rete condivise, rispetto a quelle locali/personali, per ridurre l'utilizzo di materiali di consumo (toner ed altri consumabili);
3. prediligere la stampa in bianco/nero e fronte/retro al fine di ridurre i costi, se possibile;
4. evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stampanti di rete condivise.

Nel caso in cui si rendesse necessaria la stampa di dati personali, l'utente dovrà presidiare il dispositivo di stampa per evitare la possibile perdita o divulgazione di tali informazioni e persone terze non autorizzate.

Gli scanner di rete condivisi sono configurati per poter scansionare in cartelle di rete, legate ai gruppi di lavoro. Sarà cura dell'utente cancellare, dalla cartella condivisa, i documenti scansionati una volta verificata l'attività di scansione.

L'accesso alle stampanti multifunzioni è consentito tramite l'utilizzo di PIN o altro sistema analogo di accesso. Il PIN è strettamente personale e non va mai comunicato ad altri. Non si deve inoltre utilizzare il PIN di altri utenti.

L'abilitazione degli utenti alle stampanti a colori è subordinata a formale richiesta del Dirigente del Servizio o P.O. sua delegata.

Le richieste vengono inoltrate attraverso l'apposito sistema informatico di Help Desk di assistenza del portale Intranet provinciale o in forma scritta.

12. Utilizzo memorie esterne (chiavi usb, hard disk, memory card, cd-rom, dvd, ecc.)

Di norma non devono essere utilizzate memorie esterne. Agli Utenti può essere assegnata una memoria esterna solo in casi di effettiva e motivata necessità. L'Utente è responsabile della custodia dei supporti e dei dati in essi contenuti.

Questi dispositivi devono essere utilizzati esclusivamente dalle persone a cui sono state affidate e, in nessun caso, devono essere consegnate a terzi.

1. I supporti di memorizzazione rimovibili contenenti dati sensibili o giudiziari, se non più utilizzati, devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri Utenti, solo se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili;
2. i supporti di memorizzazione rimovibili contenenti dati sensibili e/o giudiziari devono essere custoditi in idonei archivi chiusi a chiave, a cura dell'Utente che li gestisce abitualmente, e sotto sua diretta ed esclusiva responsabilità.
3. l'Utente è responsabile della custodia dei supporti e dei dati dell'Ente in essi contenuti.

È responsabilità dell'Utente cifrare il contenuto della memoria esterna in maniera tale che lo smarrimento accidentale della memoria non comporti la perdita dei dati in essa contenuti.

In caso di smarrimento/sottrazione della stessa è responsabilità dell'utente avvisare tempestivamente l'Ente dell'accaduto e del dettaglio dei dati contenuti.

È vietato collegare memorie esterne private o non autorizzate.

13. Utilizzo dispositivi di firma digitale

Ai sensi dell'art. 32, comma 1, del Codice dell'Amministrazione Digitale (CAD) gli Utenti titolari di un dispositivo di firma digitale (smart card o token USB) sono tenuti a "… assicurare la custodia del dispositivo di firma o degli strumenti di autenticazione informatica per l'utilizzo del dispositivo di firma da remoto, e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri; è altresì tenuto ad utilizzare personalmente il dispositivo di firma".

Pertanto il dispositivo di firma digitale per motivi di sicurezza deve essere custodito con la massima diligenza esclusivamente dall'Utente titolare che è l'unico a poterlo utilizzare. Non deve essere mai lasciato in custodia a terzi. Il PIN (Personal Identification Number), il codice numerico che consente all'Utente titolare di accedere alle funzioni del dispositivo di firma, è segreto e non deve essere svelato ad altri soggetti.

14. Utilizzo degli applicativi informatici

Gli applicativi informatici per la gestione informatizzata delle attività istituzionali sono strumenti di lavoro.

Il loro utilizzo è consentito previa autenticazione personalizzata e profilazione per le funzioni allo specifico applicativo.

È vietato ogni utilizzo non inerente all'attività lavorativa con la correlata responsabilità dell'Utente in ogni caso di uso illecito.

15. Rete locale provinciale

La rete informatica provinciale è una risorsa a disposizione di tutti gli utenti ed è l'infrastruttura critica per l'erogazione di tutti i servizi informatici e di telecomunicazione (compresa la telefonia fissa).

Un corretto utilizzo di questa risorsa da parte di tutti gli utenti contribuisce al buon funzionamento dei servizi erogati.

Per questo motivo è fatto divieto di collegare alla rete computer personali o computer non assegnati dal competente servizio provinciale, salvo motivata richiesta da parte del Dirigente responsabile del richiedente o P.O. sua delegata ed espressa autorizzazione da parte del Servizio Sistemi Informativi.

Per l'accesso alla rete informatica dell'Ente ciascun Utente deve essere in possesso della specifica credenziale di autenticazione.

È proibito entrare nella rete informatica e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parole chiave d'ingresso alla rete informatica ed ai programmi sono personali e vanno tenute segrete.

Le cartelle Utenti presenti nei server dell'Ente sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno temporaneamente, in queste unità. Sulle predette cartelle vengono svolte regolari attività di controllo, amministrazione e backup da parte del personale del Servizio Sistemi Informativi.

Le cartelle nominative di rete costituiscono uno spazio di lavoro temporaneo di lavoro. Per la documentazione di servizio l'utente utilizza le cartelle condivise d'ufficio.

Il personale tecnico del Servizio Sistemi Informativi è autorizzato in qualunque momento a procedere alla rimozione di ogni file o applicazione pericolosi per la sicurezza del sistema sia nei personal computer degli incaricati, sia nelle unità di rete.

È vietata l'installazione non autorizzata di dispositivi o servizi atti a trasmettere o ricevere dati che sfruttino il sistema di comunicazione telefonico per l'accesso a banche dati esterne o interne all'Ente.

È compito di ciascun Utente, per quanto di propria competenza e secondo i canoni della diligenza, preservare i dati, le notizie e le informazioni che circolano nella rete informatica dalla conoscibilità di terzi soggetti non espressamente autorizzati ad averne notizia.

È vietato monitorare ciò che transita nella rete informatica dell'Ente da parte degli Utenti.

Costituisce buona regola la periodica pulizia degli archivi (almeno ogni sei mesi), con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.

16. Rete wi-fi provinciale

Il presente documento definisce le condizioni generali di utilizzo del servizio di rete senza fili (Wireless o WiFi, denominato "servizio" nel seguito) della Provincia di Padova.

Il servizio permette la navigazione in Internet all'interno dei locali provinciali utilizzando la tecnologia Wireless.

Potranno usufruire del servizio tutti gli utenti interni ed esterni (consulenti, professionisti, tecnici e fornitori) che nell'ambito di un rapporto contrattuale con l'Ente necessitino di accedere a determinate risorse informatiche previa autorizzazione della Provincia di Padova e alle condizioni di seguito specificate. Su formale richiesta del Dirigente del Servizio o P.O. sua delegata, la richiesta delle credenziali viene inoltrata attraverso l'apposito sistema informatico di Help Desk di assistenza del portale Intranet provinciale o trasmessa in forma scritta.

Il permesso di accesso alla rete Internet tramite Wi-Fi è temporaneo e consentito solo previa autorizzazione del personale tecnico del Servizio Sistemi Informativi.

Il servizio è fornito mediante l'utilizzo di frequenze in banda condivisa e limitata protezione contro interferenza. Pertanto, l'erogazione del servizio e la sua qualità non sono garantite.

Con il primo utilizzo del servizio l'utente dichiara di aver attentamente letto ed espressamente accettato tutti i termini e le condizioni di utilizzo del servizio medesimo indicati nel presente documento, al quale dovrà attenersi scrupolosamente.

Il mancato rispetto del documento comporterà immediati provvedimenti che saranno valutati a seconda della gravità dell'azione intrapresa e della sua recidività, fino alla disabilitazione permanente dell'accesso.

L'utente riconosce che il servizio offerto dalla Provincia di Padova non garantisce in alcun modo il contenuto, la qualità, la validità di qualsiasi informazione reperita in rete.

Verrà tenuta traccia di tutte le attività svolte in rete con le credenziali dell'utente. Tali dati potranno essere messi a disposizione della Polizia Postale e dell'Autorità Giudiziaria nei casi ed alle condizioni stabilite dalla vigente normativa in materia.

La Provincia di Padova non sarà responsabile verso l'utente e/o suoi aventi causa e verso terzi per i danni diretti, indiretti o consequenziali che dovessero verificarsi per effetto di sospensioni o interruzioni del servizio.

L'utente del servizio solleva e manleva l'Amministrazione Provinciale di Padova da ogni responsabilità per eventuali danni arrecati a terzi nell'ambito del servizio e si assume la piena responsabilità per il contenuto dei messaggi trasmessi.

Non è ammesso l'accesso ai dipendenti con dispositivi privati e/o per finalità non lavorative.

16.1. Modalità di accesso al servizio

L'accesso al servizio deve essere preventivamente autorizzato previa formale richiesta del Dirigente del Servizio o P.O. sua delegata. Le richieste delle credenziali vengono inoltrate attraverso l'apposito sistema informatico di Help Desk di assistenza del portale Intranet provinciale o in forma scritta allegando fotocopia fronte-retro di documento di riconoscimento in corso di validità.

L'accesso al servizio è consentito all'utente mediante l'utilizzo di apposite credenziali, costituite da un nome utente (username) e da una parola chiave (password) che verranno rilasciate solo ed esclusivamente previa registrazione. Tali credenziali sono liberamente utilizzabili dall'utente ma, contenendo informazioni identificative, sono strettamente personali e pertanto NON cedibili.

È responsabilità dell'utente la sicurezza della custodia dei propri codici di accesso alla rete WiFi della Provincia di Padova.

La Provincia di Padova non assume alcuna responsabilità in caso di uso improprio delle credenziali di accesso.

Qualora l'utente avesse il sospetto che le proprie credenziali siano state compromesse, dovrà tempestivamente procedere alla modifica della password o, se non più possibile, segnalare l'accaduto al Settore Sistemi Informativi.

Le credenziali rappresentano la propria identità nella rete senza fili; se vengono cedute ad altri la responsabilità delle attività da costoro svolte in rete ricadrà in ogni caso sul titolare delle credenziali.

16.2. Obblighi dell'utente

L'utente del servizio è tenuto:

- Ad utilizzare il servizio nel rispetto della legislazione vigente e delle finalità per le quali è stato autorizzato (come specificato nel presente documento). In particolare, è tenuto ad osservare le leggi vigenti in materia di diritto d'autore e di protezione dei dati personali (L. 633/1941 e D. Lgs. 196/2003 e s.m.i.), nonché le specifiche norme relative al settore informatico e delle comunicazioni elettroniche;
- non connettere dispositivi mobili a titolo personale;
- a non utilizzare il servizio per effettuare comunicazioni che arrechino danni o turbative alla rete o a terzi;
- a non immettere in rete informazioni che possano presentare forme o contenuti di carattere pornografico, osceno, blasfemo, razzista, diffamatorio o offensivo;
- a non consentire l'utilizzo, a qualunque titolo, del servizio a terzi, del cui comportamento in rete si assume comunque, ai sensi del presente documento, la responsabilità;
- ad utilizzare unicamente le risorse per cui il servizio è abilitato: è possibile accedere liberamente ad Internet (Web, Posta elettronica e tutto ciò che è fruibile attraverso la rete Internet), ma non a tutti i possibili servizi esistenti online (esempio: programmi per lo scambio di file);
- a non tentare azioni di scansione della rete o attacchi alla sicurezza, espressamente vietati dalla legislazione vigente;
- a non utilizzare reti ad-hoc o altri strumenti (ad esempio sniffer) nelle aree di copertura che potrebbero influenzare negativamente le prestazioni della rete, oltre a violare il diritto alla privacy degli utenti della Provincia di Padova;
- a non configurare manualmente le impostazioni di rete del proprio PC. L'infrastruttura di accesso senza fili della Provincia di Padova assegna automaticamente indirizzo di rete e altri parametri necessari al corretto utilizzo del servizio. Impostare manualmente questi parametri può comportare malfunzionamenti della connessione per sé stessi e per altri utenti;
- a non usare in nessun caso la rete della Provincia di Padova per scaricare o scambiare materiale illegale. Lo scambio di materiale protetto da diritto d'autore (MP3, film in DivX o DVD, software commerciale, ecc.) è vietato per legge e soggetto a sanzioni penali. In caso di rilevamento di azioni illegali la Provincia di Padova procederà al richiamo formale dell'utente e metterà a disposizione delle autorità che ne facessero richiesta ai sensi di legge tutta la relativa documentazione;
- a non inviare tramite posta elettronica messaggi pubblicitari e/o promozionali o comunicazioni ad altri utenti e/o gruppi di discussione senza che sia stato richiesto ed ottenuto il relativo consenso ovvero senza che tale invio sia stato sollecitato in modo esplicito (spamming);
- a dotare il proprio PC di adeguate protezioni contro virus e altro genere di intrusioni: la Provincia di Padova non si assume alcuna responsabilità in merito ai dati contenuti nei PC degli utenti del servizio. In caso di aggressione da virus informatico o di attacco da parte di malintenzionati che dovessero in qualsiasi maniera danneggiare l'operatività

del PC o i dati in esso contenuti l'utente non potrà in alcun modo rivalersi sulla Provincia di Padova. Si invitano gli utenti a installare sul proprio PC un software antivirus efficiente ed aggiornato ed un personal firewall adeguatamente configurato.

17. Internet e social media

17.1. Internet è uno strumento di lavoro

La connessione alla rete internet dal computer o altro dispositivo informatico avuto in dotazione è ammessa esclusivamente per motivi attinenti allo svolgimento dell'attività lavorativa.

L'Utente è direttamente e pienamente responsabile dell'uso di Internet, delle informazioni che immette, delle modalità con cui opera, dei siti web o pagine Internet ai quali abbia stabilito un collegamento tramite link.

All'interno delle sedi dell'Ente possono essere rese disponibili anche reti senza fili, c.d. "Wi-Fi". Tali reti consentono l'accesso alla rete Internet e, in alcuni casi, anche alle risorse (dati) dell'Ente per i dispositivi non connessi alla rete LAN mediante cavo.

17.2. Misure preventive per ridurre navigazioni illecite

Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'Ente adotta uno specifico sistema di blocco o filtro automatico per prevenire determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una black-list.

I controlli effettuati dall'Ente a mezzo del personale tecnico del Servizio Sistemi Informativi, potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati secondo le indicazioni del Garante per la protezione dei dati personali, che prevede, relativamente alla registrazione degli accessi che devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

All'Utente inoltre non è consentito:

1. Accedere a siti internet che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico, rilevante ai fini della realizzazione di una fattispecie di reato o che siano in qualche modo discriminatori sulla base della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile;
2. salvare o installare sul proprio computer o altro dispositivo informatico programmi o archivi informatici (anche gratuiti) prelevati da siti internet o da strumenti peer to peer;
3. l'utilizzo di dispositivi personali di accesso alla rete quali modem, router 3G/4G/5G ecc. se non nei casi espressamente e formalmente autorizzati dal Servizio Sistemi Informativi;
4. l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line, mining di cripto valuta e simili salvo i casi direttamente autorizzati dall'Ente e con il rispetto delle normali procedure di acquisto;
5. ogni forma di registrazione e accesso a siti i cui contenuti non siano legati all'attività lavorativa;
6. la navigazione nei siti con contenuti pornografici e pedo-pornografici. È vietata la navigazione nei siti di giochi online;
7. la memorizzazione di documenti informatici di natura oltraggiosa, diffamatoria e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
8. accedere dall'esterno alla rete interna dell'Ente, salvo con le specifiche procedure previste dall'Ente stesso;
9. creare siti web personali sui sistemi dell'Ente nonché acquistare beni o servizi su Internet a meno che l'articolo acquistato non sia stato approvato a titolo di spesa professionale.

L'Ente al fine di rinforzare tali divieti utilizza degli strumenti informatici a protezione delle risorse informatiche.

Ogni eventuale utilizzo illegittimo di Internet, è posto sotto la personale responsabilità dell'Utente inadempiente. A seguito di ripetute e significative anomalie, l'Ente può svolgere verifiche sui dati inerenti l'accesso alla rete dei propri dipendenti. Le navigazioni saranno tracciate e conservate per il tempo strettamente limitato al perseguimento delle suddette finalità.

17.3. Partecipazioni a social media

L'utilizzo di social media dei blog e dei forum, per finalità istituzionali e/o promozionali dell'Ente deve essere preventivamente autorizzato dal Dirigente del Servizio competente, rimanendo escluse iniziative individuali da parte degli Utenti.
L'utilizzo di social media da parte dell'Utente a titolo personale e privato non può andare a scapito dell'immagine dell'Ente stesso né costituire strumento di comunicazione o diffusione di informazioni proprie dell'Ente o di cui l'Utente ha disponibilità per ragioni di lavoro.

La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni dell'Ente, nel rispetto del segreto d'ufficio, del segreto professionale e della privacy.

Al di fuori di quanto sopra indicato, resta il divieto di partecipazione ai social media durante l'orario di lavoro con gli Strumenti provinciali.

18. Posta elettronica

18.1. La Posta Elettronica

L'utilizzo della posta elettronica istituzionale è connesso allo svolgimento dell'attività lavorativa. È fatto divieto di utilizzare le caselle di posta elettronica istituzionali (nominative e/o funzionali) per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

- L'invio e/o il ricevimento di allegati contenenti fotografie, filmati o brani musicali (es. mp3) non legati all'attività lavorativa;
- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list, catene telematiche, ecc. non legati all'attività lavorativa;
- l'invio di dati particolari (sensibili);

L'assegnazione di mail nominative non implica o giustifica per quegli stessi indirizzi e-mail un carattere privato, in quanto trattasi di strumenti di esclusiva proprietà dell'Ente, messi a disposizione del dipendente al solo fine dello svolgimento delle proprie mansioni lavorative.

La posta elettronica diretta all'esterno della rete informatica provinciale può essere intercettata da estranei e, conseguentemente, non deve essere utilizzata per inviare documenti o dati di lavoro contenenti dati personali.

In caso di necessità di trasmissione, per esigenze lavorative, di "dati personali" di terzi attraverso la posta elettronica tali dati devono essere cifrati e la chiave di decifrazione deve essere comunicata attraverso un altro canale (es: telefono o sms).

La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati di dimensioni rilevanti.

Prima di aprire i file allegati ai messaggi di posta elettronica, è necessario identificare il mittente e porre particolare attenzione alla tipologia del file stesso, in caso in cui non si conosca il mittente è consigliabile procedere ad una verifica preventiva con il mittente (ad esempio tramite telefono) o eventualmente contattare il personale tecnico del Servizio Sistemi Informativi per una ulteriore verifica. Ciò al fine di evitare infezioni da virus, compromissione della propria PDL, perdita di dati personali, ecc.

Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi, questo per evitare l'infezione da virus informatici.

Al fine di garantire la funzionalità del servizio di posta elettronica e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, il sistema, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) invierà automaticamente messaggi di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto del Servizio di appartenenza. Tale funzionalità deve essere attivata dall'utente.

Gli Utenti, di norma, hanno in utilizzo indirizzi nominativi di posta elettronica strutturati con il format: nome.cognome@provincia.padova.it

Per l'assolvimento di funzioni istituzionali, su richiesta degli uffici, vengono assegnate caselle e-mail con natura impersonale (con nomenclatura del tipo: info, amministrazione, fornitori, direttore, segreteria, ragioneria ecc.). Queste caselle di servizio saranno in ogni caso associate ad una o più persone fisiche responsabili del corretto utilizzo delle stesse.

18.2. Divieti espressi

È espressamente vietato:

1. Comunicare le proprie informazioni personali o codici di accesso (nome utente, password e informazioni di sicurezza) in risposta a richieste pervenute via e-mail (phishing);
2. utilizzare l'indirizzo di posta elettronica contenente il dominio dell'Ente per iscriversi in qualsivoglia sito per motivi non attinenti all'attività lavorativa, senza espressa

autorizzazione scritta dell'Ente, nonché utilizzare il dominio dell'Ente per scopi personali;
3. creare, archiviare o spedire, anche solo all'interno della rete provinciale, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) non connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto, "catene di Sant'Antonio" o in genere a pubblici dibattiti utilizzando l'indirizzo provinciale;
4. trasmettere messaggi a tutti i dipendenti senza l'autorizzazione necessaria;
5. sollecitare donazioni di beneficenza, propaganda elettorale o altre voci non legate al lavoro;
6. simulare l'identità di un altro utente, ovvero utilizzare credenziali di posta, non proprie, per l'invio di messaggi;
7. inviare, tramite la posta elettronica, anche all'interno della rete, materiale a contenuto violento, sessuale o comunque offensivo dei principi di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico;
8. configurare l'accesso alla posta elettronica su dispositivi privati, non di proprietà dell'Ente.

18.3. Posta Elettronica in caso di assenze o cessazione

Ciascun assegnatario di un account di posta elettronica provinciale, dovrà, in caso di assenza prolungata dal servizio, attivare una funzione di risposta automatica presente nel programma di gestione della posta elettronica.

In alternativa e in tutti i casi in cui sia necessario un presidio della casella di e-mail per ragioni di operatività, l'assegnatario deve impostare il messaggio di risposta automatica di assenza comunicando i recapiti alternativi ai propri con i quali comunicare.

In caso di cessazione del rapporto di lavoro con l'Utente, la casella di posta elettronica assegnata all'utente verrà disabilitata.

Trascorsi 30 giorni dal termine del rapporto di lavoro l'Ente provvederà alla definitiva e totale cancellazione della casella di posta elettronica.

Sarà cura dell'Utente provvedere all'inserimento del messaggio di risposta automatica per avvisare gli utenti degli eventuali contatti alternativi a cui fare riferimento con congruo anticipo prima della cessazione.

19. Utilizzo sistemi in cloud

Utilizzare un servizio di cloud computing per memorizzare dati personali o sensibili, espone l'Ente a potenziali problemi di violazione delle regole sulla riservatezza dei dati personali.

È vietato agli Utenti l'utilizzo di sistemi cloud (es. Dropbox, Google Drive, Microsoft OneDrive, Apple iCloud, etc.) non espressamente approvati dall'Ente, in particolare è vietato condividere o registrare su sistemi cloud dati particolari ai sensi del Regolamento UE 679/2016 (GDPR).

L'Ente, tramite il Sevizio Sistemi Informativi, si riserva di identificare tecnologie e/o servizi cloud conformi alla normativa in materia di trattamento dei dati personali da mettere a disposizione degli Utenti.

Gli spazi di condivisione file server o cloud, devono essere utilizzati per la memorizzazione dei file ad uso strettamente lavorativo. Per la sicurezza dei sistemi, il Servizio Sistemi Informativi potrà procedere anche senza preavviso alla rimozione di file e/o applicazioni, dandone successiva e tempestiva comunicazione agli utenti.

20. Livello di Sicurezza e Strong Authentication

È necessario adeguare il livello di sicurezza informatica per l'accesso degli utenti ai servizi

dell'Ente sia dall'interno che dall'esterno della rete provinciale come indicato dall'Autorità nazionale per la cybersicurezza.

Per innalzare la sicurezza negli accessi, viene introdotta un'autenticazione forte, a due o più fattori (conosciuta anche come Strong Authentication)

L'autenticazione a due fattori richiede che l'utente utilizzi uno o più metodi di autenticazione per la verifica dell'identità che **coinvolgono anche mezzi/strumenti personali dell'utente (ad esempio cellulari smartphone e altri indirizzi email, come avviene anche per la verifica dell'identità per SPID e CIE).**

La versione 2 di SPID e CIE per accedere a tutti i portali della Pubblica Amministrazione utilizza questo tipo di autenticazione, con un'app installata sullo smartphone personale/di servizio (Possesso) e una password dell'utente (Conoscenza).

Con l'autenticazione a due fattori, dopo l'inserimento della password (primo fattore), si riceve un codice di sicurezza tramite uno o più sistemi di controllo (chiamata telefonica con voce automatica su telefono fisso o cellulare, ricezione sms, app di autenticazione installata sullo smartphone, indirizzo e-mail di appoggio personale). In alcune modalità, quando si esegue l'accesso da un nuovo dispositivo o da una nuova posizione, verrà inviato un codice di sicurezza da immettere nella pagina di accesso. A differenza della password, il codice di sicurezza (secondo fattore) è di fatto inattaccabile, in quanto generato in maniera pseudocasuale e con una durata molto limitata nel tempo che richiede l'azione dell'utente su uno o più strumenti/dispositivi a sua disposizione.

21. Formazione

L'Ente prevede sessioni formative specifiche riguardanti l'utilizzo dei sistemi informatici e la relativa sicurezza in ambito informatico. La formazione viene programmata al momento dell'ingresso in servizio, in occasione di cambiamenti di mansioni o introduzioni di rilevanti modifiche al trattamento dei dati personali.

La richiesta di formazione va inoltrata al Servizio Risorse Umane che predispone con cadenza annuale il Piano della Formazione.

22. Applicazioni e controllo

22.1. Il controllo

L'Ente, in qualità di Titolare degli strumenti informatici, dei dati ivi contenuti e/o trattati, si riserva la facoltà di effettuare i controlli indicati nel paragrafo successivo in conformità alla vigente normativa per le seguenti finalità:

1. Garantire il funzionamento dei sistemi e dei servizi informatici e di telecomunicazioni;
2. tutelare la sicurezza e preservare l'integrità degli strumenti informatici e dei dati;
3. evitare che siano commessi illeciti o per esigenze di carattere difensivo anche preventivo;
4. verificare la funzionalità del sistema e degli strumenti informatici.

Le attività di controllo potranno avvenire tramite monitoraggio, audit e/o ispezioni del sistema informatico e di tutti gli Strumenti provinciale o comunque collegati alla rete informatica. Per tali controlli l'Ente si riserva di avvalersi anche di soggetti esterni con competenze adeguate.

Tutti i controlli saranno effettuati in conformità alla normativa vigente con particolare riferimento alla normativa in materia di trattamento dei dati e dello Statuto dei Lavoratori.

22.2. Modalità di verifica

Le attività sull'uso del servizio di accesso a Internet e in generale dei servizi informatici sono automaticamente conservate in registri informatici (comunemente chiamati file di LOG) che riportano dettagli della navigazione, i siti e i documenti consultati e le operazioni verificatesi.

I file di log contengono tipicamente:

- Data ed ora dell'operazione effettuata;
- utente che ha effettuato l'operazione;
- tipologia dell'operazione effettuata;
- dati associati all'operazione effettuata.

In applicazione di quanto previsto dall'art. 5 del Regolamento Generale Sulla Protezione Dei Dati (GDPR), l'Ente promuove ogni opportuna misura organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri e, comunque, a "minimizzare" l'uso di dati riferibili agli utenti e a tale scopo ha adottato ogni possibile strumento tecnico, organizzativo e fisico, volto a prevenire trattamenti illeciti sui dati trattati con strumenti informatici.

L'Ente informa di non adottare sistemi che determinano interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura non lavorativa o privata.

In particolare eventuali sistemi atti a monitorare eventuali violazioni di legge o comportamenti anomali da parte degli Utenti avvengono nel rispetto del principio di pertinenza e non eccedenza, con esclusione di registrazioni o verifiche con modalità sistematiche.

Qualora venga rilevato un non corretto utilizzo degli Strumenti informatici messi a disposizione dall'Ente da parte dei singoli utenti, si procederà all'invio di un avviso all'utente ed al Dirigente del Servizio interessato. Sarà cura del Dirigente del Settore/Servizio interessato segnalare eventualmente l'evento al Settore Risorse Umane per l'adozione degli atti di rispettiva competenza (es. procedimenti disciplinari). Per il personale Dirigente il comportamento verrà comunicato al Segretario dell'Ente che provvederà ad inoltrare la segnalazione al competente ufficio per l'avvio del procedimento Regolamento secondo quanto previsto dalla normativa vigente.

22.3. Modalità di conservazione

I sistemi software sono stati programmati e configurati in modo da registrare nei log di sistema i dati relativi agli accessi a Internet, al traffico telematico ed alle operazioni effettuate sui sistemi informatici per un arco temporale non inferiore a 6 mesi, in funzione delle caratteristiche tecniche dell'apparato e/o dei sistemi disponibili.

Tali dati possono essere acceduti da figure tecniche istituzionalmente autorizzate ed in possesso delle opportune credenziali di accesso (a titolo esemplificativo: Amministratori di Sistema, tecnici di società esterne contrattualizzate per servizi di assistenza e manutenzione) e dall'Autorità giudiziaria in caso di presunti illeciti.

Un eventuale prolungamento dei tempi di conservazione viene valutato come eccezionale e deve aver luogo solo in relazione a:

1. Esigenze tecniche o di sicurezza, valutate a cura del Servizio Sistemi Informativi e documentate in forma scritta;
2. Indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
3. Obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

In questi casi, il trattamento dei dati personali è limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme strettamente correlate agli obblighi, compiti e finalità già esplicitati.

23. Diritti d'autore

È vietato utilizzare l'accesso ad Internet in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore (es. legge 22 aprile 1941, n. 633 e successive modificazioni, d.lgs. 6 maggio 1999, n. 169 e legge 18 agosto 2000, n. 24S). In particolare, è vietato il download di materiale soggetto a copyright (software, testi, immagini, musica, filmati, file in genere).

Non è consentito lo scarico di materiale elettronico tutelato dalle normative sul Diritto d'Autore (software, file audio, film, etc.) né attraverso Internet né attraverso servizi di "peer to peer.

24. Trattamento dei dati

24.1. Titolarità degli Strumenti e dei dati

L'Ente è esclusivo titolare degli Strumenti messi a disposizione degli Utenti ai soli fini dell'attività lavorativa. L'assegnazione, la gestione, la custodia e la dismissione di detti beni è disciplinata da procedure operative, conformi al contenuto del presente documento definite dal Servizio Sistemi Informativi e comunicate a agli Utenti.

L'Ente è l'unico esclusivo titolare e proprietario di tutte le informazioni, le registrazioni ed i dati contenuti e/o trattati mediante i propri Strumenti.

Gli Strumenti assegnati agli Utenti e restituiti dagli stessi possono essere, per esigenze organizzative, riassegnati ad altre persone all'interno dell'Ente. In questi casi il dispositivo viene formattato e ripristinato alle configurazioni iniziali appena rientrato in disponibilità.

25. Validità

25.1. Validità

Il presente Regolamento ha validità a decorrere dalla data della sua adozione.

Il Regolamento è oggetto di revisione periodica e a seguito di modifiche normative o in relazione ad eventuali evoluzioni tecniche in materia informatica e di telecomunicazioni.

Con l'entrata in vigore del presente Regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.