Disciplinare per il corretto utilizzo dei sistemi e degli strumenti informatici e telematici, della posta elettronica e della navigazione Internet

Approvato con deliberazione n. 26 del 22.09.2021

Sommario

1. – Disposizioni generali

1.1. Premessa

La crescente diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete internet dai personal computer, presta il fianco a possibili rischi per la sicurezza informatica delle risorse ICT (*Information and Communication Technology*) dell'Ente, derivanti anche da un inappropriato utilizzo degli strumenti informatici e telematici messi a disposizione dall'Ente.

Al fine di ridurre il livello di rischio e la probabilità che questo si verifichi, con conseguenti possibili danni patrimoniali, anche di immagine, il presente disciplinare pone le regole per un corretto utilizzo dei sistemi e degli strumenti informatici e telematici, della posta elettronica e della navigazione Internet.

1.2. 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.

Client: Computer o programma collegato ad un altro (computer o programma) a cui inoltra le

richieste dell'Utente.

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).

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

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

Postazione di lavoro (PDL): luogo attrezzato per svolgere un'attività lavorativa dotato di personal computer (PC) o computer portatile ed eventuali altre unità hardware.

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.

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

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 AST Bolzano.

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, altro operatore) autorizzata ad accedere alla rete informatica aziendale, ad internet e alla posta elettronica, agli applicativi aziendali e alle altre risorse informatiche e telematiche dell'Ente. Nell'ambito dell'attività assegnata tratta dati (nell'accezione definita all'interno del presente disciplinare) 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.

1.3. Finalità del disciplinare 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".

1.4. Campo di applicazione

Il presente Disciplinare 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, 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 aziendale 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.

1.5. 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 aziendali, 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 aziendali, delle applicazioni aziendali, 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 aziendali.

1.6. 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 sono disciplinate dall' Amministratore di sistema 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.

1.7. Finalità nell'utilizzo degli Strumenti e 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 aziendali.

L'Ente pertanto non potrà in ogni caso essere ritenuto responsabile per la perdita di contenuti a carattere personale (quali ad es. e-mail private, foto, documenti d'identità, file musicali, filmati ecc.).

Ogni Utente è personalmente responsabile del corretto utilizzo dei beni e delle risorse informatiche affidatigli dall'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 relazioni al proprio ruolo e alle mansioni in concreto svolte, ad operare a tutela della sicurezza informatica aziendale, riportando al proprio responsabile e al Direttore senza ritardo eventuali rischi di cui è a conoscenza ovvero violazioni del presente Disciplinare interno.

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

1.8. Compiti dell'Amministratore di Sistema

L'Ente conferisce all'Amministratore 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 aziendali.

L'Amministratore di Sistema è una figura tecnica informatica interna 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. 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 Regolamento UE 2016/679 e successiva regolamentazione D. Lgs. 101/2018;

7. 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.

1.9. 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 aziendali, 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.

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.

2. – Credenziali

2.1. Le credenziali di autenticazione

Le credenziali di autenticazione per l'accesso alla rete, ai PC ed alle applicazioni, vengono creati dall' Amministratore di Sistema, previa formale richiesta del Direttore, o suo delegato, nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente.

L'ufficio del personale è tenuto a comunicare all'Amministratore di sistema l'attivazione e la cessazione del rapporto di lavoro, nonché l'eventuale trasferimento ad altro servizio e/o mansione del dipendente/collaboratore. La comunicazione può avvenire anche con modalità automatiche.

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 dall'Amministratore di sistema, 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.

2.2. 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 può 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.

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

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

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:

1. Richiesta dell'utente per smarrimento della password
2. Richiesta di accesso al sistema con il profilo dell'utente per risoluzione di problematiche di carattere tecnico (es: malfunzionamento del software)
3. Rischio imminente di compromissione dei dati per attacco informatico
4. Richiesta dell'autorità giudiziaria
5. Interventi urgenti a protezione della rete aziendale e del funzionamento dei sistemi

2.3. Regole per la corretta gestione delle password

L'Utente, per una corretta e sicura gestione delle proprie password deve rispettare le regole seguenti:

1. Obbligo di sostituire la password assegnata al primo accesso;
2. Le password sono assolutamente personali e non vanno mai comunicate ad altri;
3. Occorre sostituire immediatamente una password non appena si abbia il dubbio che sia diventata poco "sicura" indipendentemente dalla data dell'ultimo cambio;
4. Le password devono essere lunghe almeno 8 caratteri e devono soddisfare almeno 3 dei seguenti requisiti:
    a. contenere lettere minuscole,
    b. maiuscole,
    c. caratteri speciali (ad esempio: { } [ ],.< > ; : ! " £ $ % & / ( ) = ? A \ | ' * - + _)
    d. e numeri.
5. Le password non devono essere memorizzate su alcun tipo di supporto, quali, ad esempio, Post-It (sul monitor o sotto la tastiera) o agende (cartacee, posta elettronica, telefono cellulare);
6. Le password devono essere sostituite almeno ogni 180 giorni a prescindere dall'esistenza di un sistema automatico di richiesta di aggiornamento password;
7. È vietato digitare la propria password in presenza di altri soggetti che possano vedere la tastiera, anche se collaboratori o dipendenti dell'Ente;
8. In alcuni casi, sono implementati meccanismi che consentono all'autorizzato fino ad un numero limitato di tentativi errati di inserimento della password oltre ai quali il tentativo di accesso viene considerato un attacco al sistema e l'account viene bloccato.
9. La password ideale quindi deve essere complessa, senza alcun riferimento, ma facile da ricordare.

3. – Disposizioni per l'uso delle 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 aziendali, 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 Disciplinare, a protezione della propria PDL, nel rispetto della sicurezza e dell'integrità del patrimonio aziendale.

3.1. 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 aziendale 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.

3.2. Obblighi

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

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

3.3. Modalità d'uso delle PDL dell'Ente

Il sistema informatico aziendale è composto da un insieme di unità server centrali e macchine client connesse o meno ad una rete aziendale, 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 dell'Amministratore di sistema.

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 aziendali 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.

Sentita la Direzione, l'Amministratore di sistema può in qualunque momento:

1. 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.
2. 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.

Non è consentito utilizzare aree di scambio per inviare/ricevere file se non autorizzate dalla Direzione e se non protette in lettura/scrittura con le opportune credenziali di accesso.

3.4. Corretto 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.

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;

2. In caso di allontanamento anche temporaneo dalla PDL (personal computer fisso o portatile), il dipendente non deve lasciare il sistema operativo aperto con la propria password inserita. Al fine di evitare che persone non autorizzate effettuino accessi non permessi, il dipendente deve attivare il salvaschermo con password o deve bloccare il computer (utilizzando i tasti CTRL+ALT+CANC);

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 con cui si condivide l'utilizzo dello stesso computer o a meno di necessità stringenti e sotto il proprio costante controllo.

All’Utente inoltre non è consentito:

1. Cedere in uso, anche temporaneo, le attrezzature e i beni informatici aziendali 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 aziendale.

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, 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 dall’ Amministratore di sistema dell’Ente.

3.5. 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 aziendale.

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

3.6. 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 aziendali in quanto possono essere veicolo di virus che vengono così introdotti nella rete aziendale.

È necessario contattare l'Amministratore di sistema 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).

4. – Rete locale aziendale

La rete aziendale 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 aziendale computer personali o computer non assegnati dal competente servizio aziendale, salvo motivata richiesta alla Direzione e relativa autorizzazione.

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 dell'Amministratore di sistema.

È vietata l'installazione non autorizzata di modem o altri 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'Azienda.

È compito di ciascun Utente, per quanto di propria competenza e secondo i canoni della diligenza, preservare i dati, le notizie e le informazioni aziendali 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.

5. – Internet

5.1. 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 della sede dell'Ente può essere resa disponibile anche una rete senza fili, c.d. "Wi-Fi". Tale rete consente 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.

L'accesso mediante rete Wi-Fi viene concesso a consulenti, professionisti, tecnici e fornitori che nell'ambito di un rapporto contrattuale con l'Ente necessitino di accedere a determinate risorse informatiche. Viene concesso, altresì, ai dipendenti che necessitino di svolgere compiti specifici che non possono essere svolti dalle postazioni fisse.

Il permesso di accesso alle risorse (dati) dell'Ente tramite la rete Wi-Fi può essere accordato solo dal Direttore.

Il permesso di accesso alla rete Internet tramite Wi-Fi è temporaneo e consentito solo previa autorizzazione della Direzione.

5.2. Misure preventive per ridurre navigazioni illecite

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 dall'Amministratore di sistema

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 che 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 aziendali.

Ogni eventuale utilizzo illegittimo di Internet, è posto sotto la personale responsabilità dell'Utente inadempiente.

5.3. Controlli disposti dall'azienda

1.Rispettando principi di pertinenza e di non eccedenza ed evitando una interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, così come la possibilità di controlli, costanti o indiscriminati, l'AST di Bolzano può effettuare controlli sull'uso degli strumenti elettronici, informatici e telematici aziendali.

2. Il controllo sarà svolto, in via preliminare, su dati aggregati.

3. Nell'ipotesi in cui da tale forma di controllo anonimo su dati aggregati dovesse scaturire un utilizzo anomalo degli strumenti aziendali, l'AST di Bolzano rivolgerà un invito a tutti i dipendenti di attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

4. Qualora l'anomalia dovesse ripetersi l'AST di Bolzano, dopo l'avviso di cui al comma precedente, procederà ad effettuare verifiche su base individuale sui dati inerenti all'accesso alla rete. Le navigazioni saranno tracciate e conservate per il tempo strettamente limitato al perseguimento delle suddette finalità.

5.4. 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, 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 aziendali.

5.5. Divieti di manomissione dei sistemi di sicurezza

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.

5.6. Diritto 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).

6. – Posta elettronica

6.1. La Posta Elettronica

L'utilizzo della posta elettronica aziendale è connesso allo svolgimento dell'attività lavorativa. È fatto divieto di utilizzare le caselle di posta elettronica aziendali 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:

1. l'invio e/o il ricevimento di allegati contenenti fotografie, filmati o brani musicali (es. mp3) non legati all'attività lavorativa;
2. 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;
3. l'invio di dati particolari (sensibili), es. dati sanitari.

La posta elettronica diretta all'esterno della rete informatica aziendale 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 dell'Amministratore di sistema 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 aziendale 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@bolzano-bozen.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.

6.2. Divieti espressi

È espressamente vietato:

1. Comunicare le proprie informazioni personali o codici di accesso (nome utente e password) 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 aziendale, 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 aziendale.

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 aziendale, 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.

6.3. Posta Elettronica in caso di assenze o cessazione

In caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, qualora non sia possibile attivare la funzione autoreply o l'inoltro automatico su altre caselle aziendali e si debba conoscere il contenuto dei messaggi di posta elettronica, il titolare della casella di posta può delegare, per il tempo strettamente necessario, un altro dipendente o l'Amministratore di Sistema per verificare il contenuto di messaggi e per inoltrare quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.

Sarà compito del Direttore assicurarsi che sia redatto un verbale attestante quanto avvenuto e che sia informato il lavoratore interessato alla prima occasione utile.

In caso di interruzione del rapporto di lavoro con l'Utente, l'indirizzo di posta elettronica verrà disabilitato entro un periodo massimo di 30 giorni da quella data; entro 3 mesi, invece, si disporrà la definitiva e totale cancellazione dello stesso. In ogni caso, l'Ente si riserva il diritto di conservare i messaggi di posta elettronica che riterrà rilevanti.

Eventuali dati personali contenuti nei messaggi di posta elettronica vanno salvati dall'utente prima della cessazione del rapporto di lavoro.

7. – Uso di altri Strumenti (portatile/notebook, tablet, cellulare/smartphone, dispositivi di firma digitale ed altri dispositivi elettronici)

7.1. L'utilizzo del notebook, tablet o smartphone.

Il computer portatile, il tablet e lo smartphone/cellulare (di seguito generalizzati in "dispositivi mobili") 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.

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 o a vista dentro l'auto.

Ai dispositivi mobili si applicano le regole di utilizzo previste per i computer connessi in rete e comunque tutte le policy di sicurezza previste dall'Ente.

L'Ente, per tramite dell'Amministratore di sistema, non effettua il backup dei dati memorizzati in locale sui dispositivi mobili.

Il cellulare/smartphone aziendale 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 all'attività lavorativa stessa.

I dispositivi mobili che permettono l'attivazione di una procedura di protezione PIN (Personal Identification Number devono sempre essere abilitabili solo con la digitazione del PIN stesso e non possono essere lasciati privi di PIN.

L'Utente dovrà provvedere a trasferire tutti i files creati o modificati sui dispositivi mobili sulle memorie di massa aziendali al rientro in ufficio e cancellarli in modo definitivo dai dispositivi mobili. Sui dispositivi mobili è vietato installare applicazioni (anche gratuite) se non espressamente autorizzate dall'Ente. In caso di smarrimento o furto dei dispositivi mobili deve far seguito la denuncia alle autorità competenti. Allo scopo si deve avvisare immediatamente l'Amministratore di sistema che provvederà - se del caso - ad occuparsi delle procedure connesse alla tutela dei dati.

L'Utente è tenuto comunque alla rimozione di eventuali file elaborati sui dispositivi mobili prima della riconsegna del bene.

Al fine di scongiurare i rischi derivanti dall'effetto "bridge" (ponte) tra la rete Intranet aziendale ed altre reti, gli Utenti devono evitare di accedere dall'esterno della rete Intranet ai servizi di posta elettronica aziendali e/o al servizio web aziendale e contemporaneamente ad altri siti Internet potenzialmente pericolosi.

Particolare cautela deve essere posta, inoltre, nell' utilizzo di reti WiFi gratuite per accedere alla rete Intranet e ai servizi di posta elettronica aziendale dal momento che nell'accedere a tali servizi devono essere inserite le credenziali e che queste ultime potrebbero essere facilmente carpite da malintenzionati/hacker.

7.2. Utilizzo di telefoni, scanner, stampanti e fotocopiatrici aziendali

Il telefono aziendale (fisso) assegnato all'utente è uno strumento di lavoro 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 aziendali per fini personali sia per spedire sia per ricevere documentazione.

È vietato l'utilizzo di scanner, fotocopiatrici, stampanti aziendali 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.

Le stampanti, le fotocopiatrici, gli scanner dell'Ente devono essere spenti in caso di inutilizzo prolungato.

7.3. 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 aziendali in essi contenuti.

Questi dispositivi devono essere gestiti con le stesse accortezze di cui all'articolo precedente e 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 aziendali in essi contenuti.

Qualora le memorie esterne contengano dati particolari (sensibili) e tali memorie esterne vengano portate all'esterno dell'Ente è responsabilità dell'Utente cifrare il contenuto della memoria stessa in maniera tale che lo smarrimento accidentale della memoria non comporti la perdita dei dati in essa contenuti.

7.4. 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.

7.5. Strumenti personali

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

Ai dipendenti non è permesso svolgere la loro attività lavorativa con strumentazione personale (PC fissi, portatili, tablet, smartphone) connessa alla rete aziendale.

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. In assenza di tale autorizzazione, l'utilizzo di strumenti personali deve considerarsi vietato.

7.6. Distruzione degli Strumenti

Ogni Strumento ed ogni memoria esterna affidati agli incaricati, (computer, notebook, tablet, smartphone, memory card, chiavi usb, hard disk, dvd, cd-rom, ecc.), al termine del loro utilizzo dovranno essere restituiti all' Amministratore di sistema 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.

È responsabilità dell'Utente salvare eventuali dati personali contenuti nello Strumento prima della riconsegna dello stesso all' Amministratore di sistema. L'Ente non potrà essere ritenuto responsabile per la perdita di dati personali contenuti in Strumenti aziendali.

8. – Sistemi in Cloud

8.1. Cloud Computing

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 incaricati 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 l'Amministratore di sistema, 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.

9. – Applicazione e controllo

9.1. 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 aziendali o comunque collegati alla rete aziendale. 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.

9.2. 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:

1. Data ed ora dell'operazione effettuata
2. Utente che ha effettuato l'operazione
3. Tipologia dell'operazione effettuata
4. 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 personale 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/Responsabile del Servizio interessato. Sarà cura del Responsabile del Settore/Servizio interessato segnalare eventualmente l'evento al Direttore per l'adozione degli atti di rispettiva competenza (es. procedimenti disciplinari).

9.3. 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 dall' Amministratore di sistema 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.

10. – Validità e pubblicazione

10.1. Validità

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

Il disciplinare è oggetto di revisione 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 Disciplinare tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

10.2. Pubblicazione

Il presente Disciplinare verrà pubblicato sulla intranet aziendale e diffuso a tutti i dipendenti ai sensi dell'art. 7 della legge 300/70 e del CCNL di settore.