ISTITUT LADIN "MICURÁ DE RÜ"
I - 39030 San Martin de Tor - Val Badia (BZ) Tel. (0474) 523110 - 523320 / Fax (0474) 523455
Secretariat Gherdëina: I-39048 Sëlva - Val Gherdëina (BZ) Tel. (0471) 794268 / Fax (0471) 794531

VERBAL DE RESSOLUZIUN
VERBALE DI DELIBERAZIONE
BESCHLUSSNIEDERSCHRIFT

Nr. 10/22

AL REVERDA: *Apruvazion Desposizions per co adurvé drët i strumënc ICT.*
OGGETTO: *Approvazione Disciplinare per il corretto utilizzo degli strumenti ICT.*
BETRIFFT: *Genehmigung der Verordnungen für die korrekte Benutzung der IT-Instrumente.*

L'ann *2022* ai
L'anno addì *24*
Im Jahre am

dl mëis de *11* dales
del mese di alle ore *14.30*
des Monats um Uhr

s'ál abiné le **Consëi d'Istitut**
si sono riuniti i componenti il **Consiglio d'Istituto**
haben sich di Mitglieder des **Institutsrates** versammelt.

Chisc signurs é presënc: **Castlunger dr. Elmar**
Sono presenti i signori:
Anwesend sind die Herren: **Senoner dr. Monika**
Costabiei dr. Giorgio
Moroder dr. Leander

L mancia i signurs:
Sono assenti i signori:
Abwesend sind die Herren:

Secreter:
Segretario: **Dapunt Heidi**
Sekretär:

Le Presidënt detlarëia daverta la sentada, dô ch'al á constaté le numer legal di aconsiadus,
Il Presidente, constatato il numero legale degli intervenuti, dichiara aperta la seduta
Nach Feststellung der Beschlussfähigkeit erklärt der Präsident die Sitzung für eröffnet

y prëia i presënc da to na resoluziun sön:
ed invita gli intervenuti a deliberare sul seguente oggetto:
und ersucht die Anwesenden, über folgenden Gegenstand zu beschließen:

Apruvazion Desposizions per co adurvé drët i strumënc ICT.
Approvazione Disciplinare per il corretto utilizzo degli strumenti ICT.
Genehmigung der Verordnungen für die korrekte Benutzung der IT-Instrumente.

Chësc verbal é gnû publiché sön la tofla dl Istitut.

Il presente verbale é stato pubblicato all'Albo dell'Istituto.

Diese Niederschrift wurde an der Amtstafel des Institutes veröffentlicht.

Le Secreter
Il Segretario - Der Sekretär

Urtié ala Junta Provinziala
Inviata alla Giunta Provinciale
An den Landesausschuss
übersandt

ai
il .....
am

Prot. Nr. .....

PREMESSO che con l'entrata in vigore delle nuove misure minime di sicurezza ICT per le pubbliche amministrazioni emanate da AGID, l'Istituto Ladino Micurá de Rü ha avviato un percorso di aggiornamento e rafforzamento delle proprie politiche di sicurezza informatica al fine di garantire l'integrità e la disponibilità dei dati trattati.
VORAUSGESCHICKT, dass mit Inkrafttreten der neuen, seitens der AGID erlassen, Mindestsicherheitsmaßnahmen für die öffentliche Verwaltungen, das Ladinische Kulturinstitut Micurá de Rü einen Prozess zur Aktualisierung und Stärkung seiner IT-Sicherheitsrichtlinien eingeleitet hat, mit dem Ziel die Integrität und Verfügbarkeit der verarbeiteten Daten zu gewährleisten.
METÙ DANT che cun l jì n droa dla nueva mesures minimes de segurëza ICT per l'aministrazions publiches, dat ora da AGID, l Istitut Ladin Micurá de Rü à scumencià n percurs de ajurnamënt y renfurzamënt de si politiches de segurëza nfurmatica per garantì la ntegrità y la despunibeltà di dac tratà.

PREMESSO che al fine di rafforzare la sicurezza ICT è necessario anche che tutti i soggetti che a vario titolo accedono alla rete informatica aziendale dell'Istituto Ladino Micurá de Rü (dipendenti, collaboratori, fornitori, etc.) si conformino a regole di comportamento ed utilizzo di strumenti informatici che non determinino un potenziale rischio per la sicurezza dei dati trattati.
VORAUSGESCHICKT, dass es zur Stärkung der IT-Sicherheit auch erforderlich ist, dass alle Subjekte, welche aus verschiedenen Gründen auf das Unternehmens-IT-Netzwerk des Ladinischen Kulturinstitutes Micurá de Rü zugreifen (Angestellte, Mitarbeiter, Lieferenten, usw.), Verhaltensregeln einhalten und IT-Tools verwenden, die kein potenzielles Risiko für die Sicherheit der verarbeiteten Daten darstellen.
METÙ DANT che per renfurzé la segurëza ICT iel nce debujën che duta la persones, nfat a ce titul che les ruva permez ala rë nfurmatica dl Istitut Ladin Micurá de Rü (dependënc, culaburadëures, furnitëures, i.n.i.), se tënie a regules de cumpurtamënt y de adurvanza de strumënc nfurmatiches che ne porte nia n risch putenziel per la segurëza di dac tratei.

ESAMINATO il nuovo "Disciplinare per il Corretto Utilizzo degli Strumenti Informatici e Telematici Internet e posta elettronica, redatto dall'Ufficio Privacy,
NACH PRÜFUNG der neuen „Verordnungen für die korrekte Verwendung von IT-und Telematik-Tools und E-mails, die vom Datenschutzbüro entworfen wurden,
EJAMINEDES che la nueva „Despusizions per co adurvé drët i strumënc nfurmatics y telematics y la posta eletronica, elaburà dal ufize protezion dac,

SU PROPOSTA del Presidente, all'unanimità di voti favorevoli legalmente espressi, il Consiglio d'Istituto
AUF VORSCHLAG des Präsidenten, mit gesetzmäßig zum Ausdruck gebrachter Stimmeneinhelligkeit
SÖN PROPOSTA dl Presidënt, cun l'unanimité dles usc consenziëntes pronunziades legalmënter,

d e l i b e r a
b e s c h l i e ß t
d e l i b e r ë i a

der Institutsrat.

le Consei d'Istitut,

1. di approvare l'allegato Disciplinare per il Corretto Utilizzo degli Strumenti Informatici e Telematici Internet e posta elettronica", quale parte integrante e sostanziale del presente atto.
   die beigefügten Verordnungen für die korrekte Verwendung von IT-und Telematik-Tools und E-mails, als integralen und wesentlichen Bestandteil dieser Beschlussniederschrift, zu genehmigen.
   de apruvé la despusizions per co adurvé drët i strumënc nfurmatics y telematics y posta eletronica tlo njuntedes, sciche pert ntegreda y sustanziela de chësta delibera.
2. di pubblicare sul sito aziendale il Disciplinare e darne massima diffusione ai dipendenti e fornitori di beni e servizi dell'Istituto Ladino.
   die Verordnungen auf der Unternehmenswebseite des Ladinischen Kulturinstitutes, zu veröffentlichen und best möglichst unter den Mitarbeitern und Lieferanten von Waren und Dienstleistungen des Ladinischen Institutes, zu verbreiten.
   de publiché sun l sit dla firma la despusizions y cialé de les fé cunëscer plu che la va danter y dependënc y furnitëures de bëns y servijes.

Dô che chësc verbal é gnü lit, él gnü aprové y sotescrit.
Data lettura del presente verbale, viene approvato e sottoscritto.
Nach Vorlesung wird diese Niederschrift genehmigt und unterzeichnet.

Le Presidënt - Il Presidente - Der Präsident La Secreteria-La Segretaria - Die Sekretärin

dr. Elmar Castlunger *Heidi Dapunt*

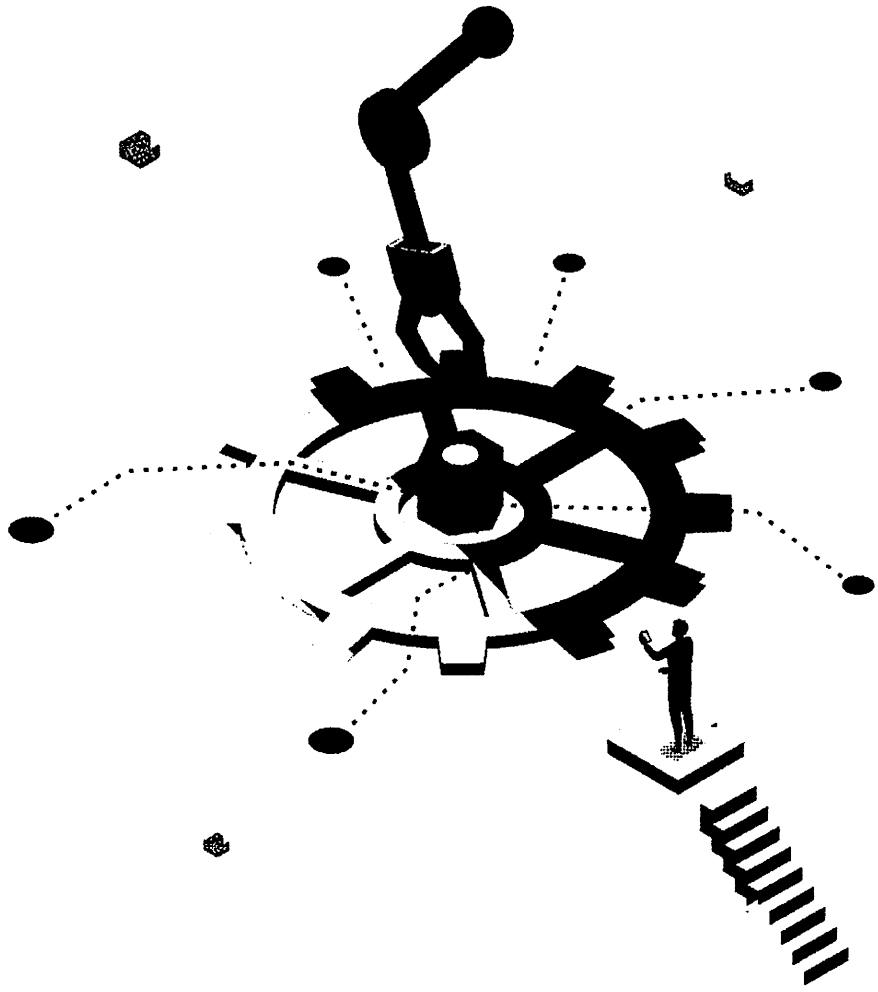
Por copia te döt anfat al original, relasciada sön cherta nia bolada por pratighes d'aministraziun.
Per copia conforme all'originale, rilasciata in carta libera per uso amministrativo.
Für die Übereinstimmung mit der Urschrift, ausgestellt auf stempelfreiem Papier für Verwaltungszwecke.

ai – lí – am

Odü: **Le Presidënt**
Visto: **Il Presidente** - Gesehen: **Der Präsident** **La Secreteria- La Segretaria - Die Sekretärin**

dr. Elmar Castlunger *Heidi Dapunt*

San Martin de Tor (BZ)www.micura.it
Val Badia info@micura.it
Sëlva (BZ) T +39 0471 794 268 Cod.fisc. 81008440216
Gherdëina info.gh@micura.it Part.CVA 01089600215



Disciplinare per il corretto utilizzo degli strumenti ICT

Versione n. 1/2022

Approvato dl ISTITUT LADIN MICURA' DE RÜ in data 24.11.2022

Il presente Disciplinare è stato predisposto dall'Istitut Ladin Micurá de Rü. ai sensi e per gli effetti del Regolamento (UE) 2016/679 e delle linee guida dell'Autorità Garante per posta elettronica e internet (G.U. n. 58 del 10 marzo 2007)

Sommario

**Nel presente documento, l'uso del genere maschile per indicare i soggetti, gli incarichi e gli stati giuridici è utilizzato solo per esigenze di semplicità del testo ed è da intendersi riferito a entrambi i generi.*

Glossario

Amministratore di Sistema (di seguito, per brevità, ADS): con la definizione di "amministratore di sistema" si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti.

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.

Autorità Garante per la Protezione dei Dati Personali: (di seguito, per brevità, GPDP) autorità amministrativa indipendente istituita dalla L. 31 dicembre 1996, n. 675, poi disciplinata dal Codice Privacy (D.lg. 30 giugno 2003 n. 196), come modificato dal D.lgs 10 agosto 2018, n. 101. Quest'ultimo ha confermato che il GPDP è l'autorità di controllo nazionale, designata ai fini dell'attuazione dell'art. 51 del Regolamento (UE) 2016/679.

Bring Your Own Device (BYOD): (di seguito, per brevità BYOD)» è un'espressione usata per riferirsi all'utilizzo dei propri dispositivi personali (es. PC, tablet, cellulari privati) nel posto di lavoro, e usarli per avere gli accessi privilegiati alle informazioni del Titolare e alle loro applicazioni.

Cloud Computing: paradigma di erogazione di risorse informatiche, come l'archiviazione, l'elaborazione o la trasmissione di dati, caratterizzato dalla disponibilità on demand attraverso Internet a partire da un insieme di risorse preesistenti e configurabili.

Data Breach: violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato/a); 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.

Dispositivi di memoria portatili: tutti quei dispositivi che consentono di copiare o archiviare dati, files, o documenti esternamente al computer (es. cd-rom, dvd, pen-drive USB, riproduttori musicali mp3, fotocamere digitali, dischi rigidi esterni, ecc.).

Informazioni riservate: tutte le informazioni acquisite dall'Utente, che non siano di pubblico dominio, fornite per iscritto, in formato elettronico o in qualsiasi altra forma e/o supporto.

Malware: qualsiasi programma informatico usato per disturbare le operazioni svolte da un Utente di un computer.

Postazione di lavoro: complesso unitario di personal computer, notebook, tablet, smartphone, accessori, periferiche e ogni altro dispositivo concesso all'Utente o utilizzato dal medesimo in modalità BYOD.

Risorse informatiche: qualsiasi strumento disponibile in un computer (o altro dispositivo) utilizzato dall'Utente nei processi di elaborazione (hardware e software).

Sistema informativo: insieme delle informazioni utilizzate, prodotte e trasformate da un'azienda durante l'esecuzione dei processi aziendali, dalle modalità in cui esse sono gestite e dalle risorse sia umane sia tecnologiche coinvolte.

Smart Working: una modalità di esecuzione del rapporto di lavoro subordinato caratterizzato dall'assenza di vincoli orari o spaziali e un'organizzazione per fasi, cicli e obiettivi, stabilita dal datore di lavoro.

Strumenti di lavoro: tutti quei dispositivi utilizzati in via primaria ed essenziale per l'esecuzione dell'attività lavorativa ovvero direttamente preordinati all'esecuzione della prestazione lavorativa.

Trattamento di dati personali: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Utente: lavoratore, dipendente, collaboratore, consulente esterno, volontario, altro operatore autorizzato ad accedere alla rete informatica aziendale, a internet e alla posta elettronica, agli applicativi ed alle altre risorse informatiche e telematiche di proprietà del Titolare, a prescindere dal rapporto contrattuale in essere tra le parti. Tale figura sarà anche indicata quale "autorizzato del trattamento" nell'accezione propria dell'art. 29 del Regolamento (UE) 2016/679.

Premessa

Il presente Disciplinare si pone l'obiettivo di definire l'ambito di applicazione, le modalità e le norme sul corretto utilizzo della strumentazione da parte del personale (di seguito "Utenti") al fine evitare condotte, anche inconsapevoli, che potrebbero esporre lo stesso a problematiche di sicurezza, di immagine nonché patrimoniali per danni cagionati anche a terzi e fornire le regole per la tutela della riservatezza, integrità e disponibilità dei dati personali trattati nello svolgimento della propria mansione.

La progressiva diffusione delle tecnologie nella società dell'informazione espone i Titolari del trattamento a possibili rischi: "anche Tu puoi contribuire ad evitare tali rischi"

Il trattamento dei dati personali, svolto mediante strumenti cartacei ovvero informatici, deve essere improntato all'osservanza dei principi sanciti dalla vigente normativa in materia di protezione dei dati personali. In particolare, dovrai:

1. trattarli in **modo lecito, corretto e trasparente**;
2. raccoglierli per **finalità determinate, esplicite e legittime**;
3. trattarli in **maniera adeguata, pertinente e limitata** a quanto necessario rispetto alle finalità per le quali sono trattati;
4. **conservarli per un arco temporale** non superiore al conseguimento delle finalità per le quali sono trattati;

garantire una adeguata sicurezza dei dati personali, mediante misure di sicurezza tecniche ed organizzative adeguate, evitando trattamenti non autorizzati o illeciti e dalla perdita, distruzione o danno accidentale.

Per ogni necessità o chiarimento può **contattare il Titolare al seguente indirizzo e-mail: leander@micura.it**

1. Ambito di applicazione e quadro normativo di riferimento

Il presente Disciplinare si applica ad ogni assegnatario di beni e risorse informatiche ovvero utilizzatore di servizi e risorse informatiche ed informative messi a disposizione dal Titolare nonché ad ogni Utente che – previa autorizzazione del Titolare – utilizza dispositivi propri o privati (BYOD) per finalità connesse allo svolgimento dell'attività lavorativa.

Il Disciplinare, per quanto compatibile, si applica altresì al personale che svolge la propria attività lavorativa in Smart Working o da remoto.

Il presente Disciplinare è stato adottato sulla base seguenti disposizioni:

- Deliberazione n. 13 del 1º marzo 2007 (G.U. n. 58 del 10 marzo 2007) del GPDP recante "trattamento dei dati personali relativo all'utilizzo di strumenti informatici da parte dei lavoratori";
- L. 22 maggio 2017, n. 81 recante "misure per la tutela del lavoro autonomo non imprenditoriale e misure volte a favorire l'articolazione flessibile nei tempi e nei luoghi del lavoro subordinato";
- D.M. 19 ottobre 2020 recante "misure per il lavoro agile nella pubblica amministrazione nel periodo emergenziale";
- (ove applicabile) D.L. 7 marzo 2005, n. 82, c.d. Codice dell'Amministrazione Digitale (CAD);
- Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali;
- D.L. 10 agosto 2018, n. 101 che reca le disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679.

2. Gestione degli strumenti ICT

Il Titolare, in base al ruolo ricoperto e alla mansione svolta, valuta la presenza dei presupposti per l'autorizzazione all'uso e all'affidamento e definisce le regole per l'utilizzo dei seguenti strumenti di lavoro:

☐ Accesso alla rete internet – Wi-Fi
☐ Personal Computer
☐ Smartphone e Tablet
☐ Telefonia fissa
☐ Indirizzo di posta elettronica
☐ Indirizzo di posta elettronica certificata (PEC)
☐ Chiavetta USB e altri strumenti per l'archiviazione esterna della documentazione
☐ Software installati sul dispositivo affidato dal Titolare
☐ Altro [redacted]

I dispositivi sopra assegnati sono strumenti di lavoro e non potranno essere utilizzati in nessun caso per finalità personali o private, salvo espressa autorizzazione scritta dal Titolare. Gli strumenti di lavoro ed i dati contenuti o trattati mediante tali strumenti sono da considerarsi di proprietà del Titolare.

L'Utente non è autorizzato in alcun modo alla modifica delle caratteristiche degli strumenti di lavoro. In caso di anomalie, si raccomanda ad informare tempestivamente il Titolare.

Previa autorizzazione dal Titolare, ove applicabile, l'Utente potrà utilizzare un dispositivo di proprietà (BYOD) per lo svolgimento della prestazione lavorativa in Smart Working o da remoto. L'Utente dovrà garantire sempre e comunque un ambiente d'uso rispondente a misure di sicurezza analoghe a quelle previste per l'utilizzo degli strumenti di lavoro messi a disposizione dal Titolare.

L'Ufficio IT-interno potrà eseguire interventi sui dispositivi assegnateli per esigenze di manutenzione, aggiornamento o implementazione di programmi e/o misure di sicurezza volti a tutelare i dati e le informazioni trattate. In nessun caso tali

interventi avranno come obiettivo il controllo dell'attività lavorativa eseguita dall'Utente quanto piuttosto verificare o migliorare la sicurezza delle informazioni nell'utilizzo degli strumenti di lavoro.

3. Postazione di lavoro

L'accesso alle postazioni di lavoro da parte dell'Utente deve avvenire mediante *login*. L'Utente dovrà inserire *Username* e *Password* per aprire una sessione di lavoro.

Ove previsto, potrà essere assegnato un univoco *Username* e *Password* per gruppi di Utenti per l'accesso alla postazione di lavoro. Rimarranno invece separati ed univoci *username* e *password* per l'accesso agli applicativi (es. posta elettronica).

Al termine di ogni sessione di lavoro, tutte le applicazioni devono essere chiuse tramite *logout* in quanto la non corretta chiusura può comportare una perdita di dati o l'accesso agli stessi da parte di soggetti terzi non autorizzati.

4. Personal Computer (PC) fissi e portatili

Il Titolare può affidare all'Utente, in comodato d'uso (ex art. 1803 e ss. del c.c.), per tutta la durata del periodo della prestazione, il PC quale strumento di lavoro.

L'accesso al PC deve essere protetto da *username* e *password* custoditi dall'Utente con la massima diligenza e non divulgata a soggetti terzi. Per accedere al PC l'Utente dovrà ogniqualvolta identificarsi tramite *login* con il proprio *username* e *password*.

Se ti allontani dalla postazione di lavoro metti in protezione il PC (modalità screen saver) affinché persone non autorizzate non abbiano accesso ai dati!

Mediante lo scambio di file via internet (es. tramite e-mail, supporti removibili, *file-sharing*, chat, ecc.) possono essere trasmessi virus informatici in grado di danneggiare gli strumenti di lavoro e sottrarre i dati ivi contenuti. Senza preventiva autorizzazione scritta del Titolare è fatto divieto all'Utente di eseguire le operazioni seguenti:

a) gestire, memorizzare, trattare file, documenti e/o informazioni personali o comunque non afferenti alle attività lavorative – anche temporaneamente – nella rete locale, nel disco fisso o in altri supporti di massa;

b) modificare le configurazioni del PC preimpostate dal Titolare;

c) installare software o applicazioni ulteriori rispetto a quelle presenti sul PC (es. software senza licenza e/o versione diversa, anche più recente rispetto a quelle fornite con il dispositivo);

d) aggiungere o collegare dispositivi hardware (es. hard disk, memorie USB, CD, DVD, ecc.) o periferiche (es. telecamere, fotocamere, smartphone, webcam, ecc.).

Si raccomanda, inoltre, di:

a) non caricare sul disco fisso del PC documenti, giochi, file di musica, materiale audiovisuale (es. foto, video) non inerenti allo svolgimento dell'attività lavorativa;

b) non effettuare autonomamente attività manutentive del PC o affidarle a soggetti terzi non autorizzati;

c) non installare autonomamente antivirus, anti-malware e firewall;

d) non disattivare l'antivirus, anti-malware e firewall fornito dal Titolare, anche temporaneamente, e verificarne periodicamente il corretto funzionamento;

non conservare documenti lavorativi sul desktop del PC, salvo necessità di lavorazione temporanea dello stesso in quanto il desktop del PC non è sottoposto a *backup* e in caso di problematica i documenti ivi collocati potrebbero andare smarriti

senza possibilità di recupero. Per tale ragione tutti i documenti di carattere lavorativo andranno collocati nei luoghi sottoposti a salvataggio e *backup* (*server*).

Ricordati di comunicare ç ogni anomalia o malfunzionamento del PC e dei sistemi antivirus, anti-malware nonché la presenza di virus o file sospetti e di ogni altra attività sospetta al Titolare

Per quanto concerne i PC portatili si applicano le regole di utilizzo in genere previste per i PC fissi. L'Utente è responsabile del PC portatile e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo (ove applicabile anche in modalità Smart Working). In caso di viaggi il PC deve essere sempre trasportato come bagaglio a mano e sistemato in una custodia adeguata. Si raccomanda, inoltre, di non lasciare incustodito il PC (es. in auto durante le soste nelle stazioni di servizio oppure durante la pausa pranzo presso clienti, ecc.).

5. Telefonia fissa e mobile

Il telefono fisso, così come lo smartphone e/o il tablet, qualora assegnati, sono strumenti di lavoro.

Non sono consentite comunicazioni a carattere personale tramite questi strumenti di lavoro, salvo in casi di necessità ed urgenza.

Al fine di un corretto utilizzo di tali strumenti di lavoro è necessario osservare le seguenti regole.

a) I dispositivi di telefonia (smartphone) devono essere dotati di password di sicurezza (es. codice PIN del dispositivo) che ne impedisca l'utilizzo da parte di altri soggetti. A tal fine si precisa che:

   - ✓ il codice PIN dovrà essere composto da 4-5 cifre numeriche. Altri codici di accesso dovranno garantire analoga protezione;
   - ✓ il codice PIN o altri codici di accesso dovranno essere modificati dall'Utente al momento della consegna dello strumento di lavoro e con cadenza al massimo semestrale;
   - ✓ ogni utente deve adottare le necessarie e dovute cautele per assicurare la segretezza della password e, qualora ritenga che un soggetto non autorizzato possa esserne venuto a conoscenza, dovrà provvedere immediatamente a cambiarla dandone comunicazione al Titolare;

b) in caso di furto, danneggiamento o smarrimento del dispositivo l'assegnatario dovrà darne immediato avviso al Titolare: se tali eventi sono riconducibili a un comportamento negligente o imprudente dell'assegnatario stesso o comunque a sua colpa nella custodia, lo stesso sarà ritenuto unico responsabile dei danni derivanti;

c) in caso di furto o smarrimento, il Titolare si riserva la facoltà di attuare la procedura di cancellazione da remoto di tutti i dati sul dispositivo, rendendo il dispositivo stesso inutilizzabile e i dati in esso contenuti del tutto irrecuperabili;

d) non è consentito caricare qualsiasi dato personale non attinente all'attività lavorativa svolta o inserire all'interno del dispositivo una SIM diversa da quella data in dotazione dal Titolare;

e) non è consentito effettuare riprese, fotografie, registrazioni di suoni, salvo che per necessità lavorative e previa autorizzazione scritta del Titolare;

f) l'installazione di applicazioni, gratuite o a pagamento, deve essere espressamente autorizzata, rimanendo in caso contrario a carico dell'Utente le responsabilità derivanti dall'installazione non autorizzata;

g) al momento della consegna, l'Utente è tenuto a verificare la disattivazione del sistema di geolocalizzazione potenzialmente attivabile sugli smartphone e tablet, consapevole che in caso contrario il Titolare potrebbe venire

a conoscenza, seppur incidentalmente, dei dati relativi alla posizione del dispositivo stesso e del suo assegnatario. In ogni caso, tale rilevazione non avrà come obiettivo il controllo dell'attività lavorativa eseguita dall'Utente;

h) lo smartphone, dovrà risultare acceso nel corso di tutto l'orario in cui il lavoratore presta la propria attività lavorativa, o per tempi più lunghi, secondo gli orari concordati con il datore di lavoro.

L'Utente dovrà rispettare le soglie di traffico previste dal piano tariffario siglato con l'operatore, sia per quanto attiene al traffico telefonico che al traffico dati eseguito tramite utilizzo delle applicazioni o attraverso la navigazione. Il dettaglio specifico delle soglie di traffico previste dall'operatore, verrà indicato nella lettera di assegnazione della scheda SIM. Il Titolare potrà eseguire verifiche periodiche per accertare il rispetto di dette soglie.

6. Utilizzo della posta elettronica

L'utilizzo della posta elettronica, anche certificata (PEC), è connesso allo svolgimento dell'attività lavorativa. È, pertanto, vietato l'uso per motivi personali. Gli Utenti sono inoltre responsabili del corretto utilizzo delle caselle di posta elettronica e delle comunicazioni effettuate e ricevute, anche per quanto attiene la riservatezza dei dati ivi contenuti, la cui diffusione impropria potrebbe configurare violazione del segreto d'ufficio e dalla vigente normativa sulla protezione dei dati personali. Sono vietati, dunque, i comportamenti che possano creare un danno – anche d'immagine – al Titolare.

Nonostante la possibile presenza nella strutturazione dell'indirizzo e-mail, di elementi identificativi della persona, quali ad esempio nome e cognome (nome.cognome@ragionesociale.it), la casella e-mail resta di proprietà del Titolare, che ne concede l'utilizzo.

In caso di assenze programmate, vengono messe a disposizione dell'Utente apposite funzionalità che consentono di inviare risposte automatiche contenenti le coordinate di altro soggetto cui trasmettere le comunicazioni e-mail di contenuto lavorativo o altre utili modalità di contatto.

In caso di assenze non programmate (es. per malattia o infortunio), qualora il lavoratore non possa attivare la procedura sopra descritta, il Titolare potrà disporre mediante personale incaricato o tramite l'Amministratore di Sistema l'attivazione di una risposta automatica avvertendo l'assenza.

Nel caso in cui il Titolare necessiti di conoscere il contenuto dei messaggi di posta elettronica dell'Utente resosi assente – per cause improvvise o per improrogabili necessità legate all'attività lavorativa – il Titolare o l'Amministratore di Sistema (ove nominato), potrà accedere alla casella e-mail al fine di estrapolare eventuali comunicazioni necessarie per proseguire con le attività lavorative.

In caso di interruzione del rapporto di lavoro, l'indirizzo di posta elettronica verrà disabilitato entro un periodo massimo di 30 giorni. Entro 90 giorni, il Titolare disporrà la definitiva e totale cancellazione dello stesso. In ogni caso, il Titolare si riserva il diritto di conservare i messaggi di posta elettronica ritenuti rilevanti per il proseguimento dell'attività lavorativa. Anche in questo caso, il Titolare potrà predisporre idoneo risponditore automatico, volto ad informare i mittenti circa l'avvenuta interruzione del rapporto di collaborazione professionale.

Per un corretto utilizzo della posta elettronica è fatto divieto di eseguire le seguenti operazioni:

a) utilizzare la casella di posta elettronica per finalità commerciali estranee e diverse rispetto all'attività eseguita dal Titolare;

b) utilizzare l'indirizzo e-mail per trasmettere o scambiare materiale illecito o coperto da diritto d'autore ed in generale non può contenere informazioni non pertinenti rispetto all'attività lavorativa eseguita

c) utilizzare l'indirizzo e-mail per registrare account a siti i cui contenuti non siano legati all'attività lavorativa

È altresì opportuno inserire in calce alla firma della e-mail un disclaimer per i destinatari:

"Le informazioni contenute nel presente messaggio ed i relativi allegati sono riservate e confidenziali e comunque destinate esclusivamente alle persone o ai soggetti indicate come destinatari, pertanto ne è vietata la diffusione, la comunicazione, la distribuzione o la copia da parte di qualsiasi soggetto diverso dal destinatario. Qualora Lei non fosse la persona al quale il presente messaggio è destinato La invitiamo, dopo aver tempestivamente informato il mittente, ad eliminarlo e a non utilizzarne in alcun caso il contenuto. Qualsiasi utilizzo non autorizzato di questo messaggio e dei suoi eventuali allegati espone a conseguenze civili e penali".

7. E-mail phishing

Il phishing è una tecnica illecita utilizzata per appropriarsi di informazioni riservate relative a una persona o a un'azienda - username e password, codici di accesso (come il PIN del cellulare), numeri di conto corrente, dati del bancomat e della carta di credito – con l'intento di compiere operazioni fraudolente.

La truffa avviene di solito via e-mail, ma possono essere utilizzati anche sms, chat e social media. Il "ladro di identità" si presenta, in genere, come un soggetto autorevole (es. banca, gestore di carte di credito, pubblica amministrazione, ecc.) che invita a fornire dati per risolvere particolari problemi tecnici con il conto bancario o con la carta di credito, per accettare cambiamenti contrattuali o offerte promozionali, per gestire la pratica per un rimborso fiscale o una cartella esattoriale, ecc.

Presta la massima attenzione ai messaggi di posta elettronica provenienti da mittenti di cui non si conosce con certezza l'identità o destano particolari sospetti in ordine al contenuto.

A volte, i messaggi di phishing invitano a fornire, direttamente, i propri dati personali oppure a cliccare un link che rimanda ad un sito web dove è presente un *form* da compilare. Spesso dietro i nomi di dominio dei siti web apparentemente sicuri o le URL abbreviate che si trovano sui social media si nascondono link a contenuti non sicuri.

L'Utente, vittima di un tentativo di phishing, è tenuto a segnalarlo immediatamente al Titolare onde evitare danni maggiori.

8. Utilizzo della rete internet e wi-fi

La connessione alla rete internet o alla rete wi-fi è ammessa solo per motivi attinenti allo svolgimento dell'attività lavorativa. L'Utente è responsabile per la navigazione e per le operazioni eseguite nel corso della consultazione dei siti web.

L'utilizzo della rete Wi-Fi tramite dispositivi personali potrà avvenire unicamente previa autorizzazione. L'accesso è subordinato all'inserimento di Username e Password.

Il Titolare potrà adottare idonee misure tecniche preventive volte a ridurre navigazioni a siti non correlati all'attività lavorativa attraverso filtri e black list.

Per un corretto utilizzo della rete internet, salvo autorizzazione specifica da parte del Titolare, è fatto divieto di eseguire le seguenti operazioni:

a) accedere a siti internet vietati mediante azioni inibenti dei filtri, sabotando o comunque superando o tentando di superare o disabilitando i sistemi adottati dal Titolare per bloccare accessi non conformi all'attività lavorativa;

b) accedere dall'esterno alla rete locale;

c) partecipare a *forum* non professionali, utilizzare chat e bacheche elettroniche, partecipare a gruppi di discussione o lasciare commenti ad articoli o iscriversi a mailing list spendendo il nome del Titolare e/o per scopi privati;

d) scaricare materiale soggetto a *copyright* (es. testi, immagini, musica, filmati, ecc.) in violazione della vigente normativa sul diritto di autore;

e) utilizzare social network (es. Facebook, Instagram, LinkedIn, ecc.);

f) utilizzare la rete internet per scaricare materiali quali film, musica, libri, immagini o software. Laddove in ragione dell'attività lavorativa, risulti necessario utilizzare un software gratuito scaricabile dalla rete, l'utente dovrà darne comunicazione al Titolare, che se del caso, procederà all'installazione del software indicato.

9. Gestione delle password

Le password costituiscono il metodo di autenticazione più idoneo per garantire l'accesso agli strumenti di lavoro.

Per una corretta e sicura gestione delle proprie password è necessario attuare le seguenti pratiche:

a) impostare una password di almeno 8 caratteri. Più aumenta il numero dei caratteri più la password diventa "sicura" (si suggerisce intorno ai 15 caratteri);

b) inserire caratteri di almeno 4 diverse tipologie, da scegliere tra: lettere maiuscole, lettere minuscole, numeri, caratteri speciali (es. punti, trattino, underscore, ecc.);

c) evitare i riferimenti personali facili da indovinare (es. nome, cognome, data di nascita, ecc.). Non deve nemmeno contenere riferimenti al nome utente (detto anche user account, alias, user id, username);

d) evitare l'utilizzo delle parole "da dizionario", cioè parole intere di uso comune. È meglio usare parole di fantasia oppure parole "camuffate" per renderle meno comuni, magari interrompendole con caratteri speciali (es. caffè può diventare caf-f3). Esistono infatti software programmati per tentare di indovinare e rubare le password provando sistematicamente tutte le parole di uso comune nelle varie lingue, e con questa accortezza si può rendere il loro funzionamento più complicato;

e) cambiare periodicamente le password, soprattutto per i profili più importanti o quelli che usi più spesso (es. e-mail, e-banking, social network, ecc.).

L'Utente è pregato di non scrivere le password su foglietti di carta lasciati sul posto di lavoro, onde evitare che altre persone le possano leggere.

10. Dispositivi di memoria portatili/removibili

Senza previa autorizzazione scritta del Titolare è vietato utilizzare supporti rimovibili personali. Se autorizzati in base alle procedure previste, una volta connessi all'infrastruttura informatica del Titolare, i dispositivi saranno soggetti (ove ciò sia compatibile) al presente Disciplinare.

Custodisci i dispositivi di memoria portatili in modo adeguato onde evitare che il loro contenuto possa essere trafugato, alterato o distrutto

Il supporto di archiviazione non deve essere mai lasciato incustodito, e se trasportato all'esterno della sede di lavoro, andrà prestata particolare attenzione alla sua custodia. Nello specifico:

a) i supporti di archiviazione, smarriti e/o accidentalmente lasciati incustoditi, anche per breve periodo, possono essere rapidamente letti e copiati, senza lasciare alcuna traccia dell'accaduto;

b) il contenuto del supporto removibile deve essere cancellato quando non più necessario allo svolgimento dell'attività lavorativa;

c) non è consentito caricare sul supporto documenti informatici in supporti removibili non aventi alcuna attinenza con la propria prestazione lavorativa.

11. Stampanti, fax e distruggi documenti

L'utilizzo delle stampanti ovvero del fax deve avvenire sempre per scopi professionali. Non è consentito l'utilizzo per uso privato salvo specifica autorizzazione da parte del Titolare.

Si raccomanda di non lasciare le stampe incustodite e ritirare immediatamente le copie appena stampate.

Quando invii documenti contenenti dati personali o informazioni riservate su una stampante condivisa è richiesta una particolare attenzione al fine di evitare che persone non autorizzate possano venire a conoscenza del contenuto della stampa

L'utilizzo di fax per l'invio di documenti che hanno natura strettamente confidenziale è generalmente da evitare. In caso ciò sia necessario si deve preventivamente avvisare il destinatario in modo da ridurre il rischio che persone non autorizzate possano venire a conoscenza del contenuto della comunicazione e successivamente chiedere la conferma telefonica di avvenuta ricezione.

I distruggidocumenti sono da utilizzare nel caso in cui documenti cartacei contenenti dati personali non siano più necessari, così da evitarne la presa visione o l'impossessamento da parte di soggetti terzi non autorizzati.

12. Gestione dati raccolti mediante supporti cartacei (Clean Desk Policy)

Allo scopo di migliorare la sicurezza e la riservatezza dei dati trattati e al fine di ridurre il rischio di perdita e danneggiamento di informazioni durante e al di fuori dell'orario di lavoro o quando le aree di lavoro non sono presidiate è necessario attenersi alle seguenti regole:

a) non lasciare in vista sulla propria scrivania dati raccolti mediante supporti cartacei quando ci si allontana dalla postazione di lavoro oppure quando è previsto un incontro con un soggetto non abilitato alla conoscenza dei dati in essi contenuti;

b) prima di lasciare la postazione di lavoro, anche per brevi periodi (es. durante la pausa pranzo o durante una riunione), è obbligatorio riporre in luogo sicuro i dati raccolti e trattati mediante supporti cartacei;

c) a fine giornata lavorativa l'Utente deve provvedere al riordino della scrivania e alla corretta archiviazione di tutti i documenti lavorativi;

d) i documenti lavorativi devono essere debitamente conservati (es. in appositi armadi chiusi a chiave) quando non sono in uso, soprattutto al di fuori dell'orario di lavoro;

e) i documenti devono essere eliminati dall'Utente, quanto non più necessari per lo svolgimento dell'attività lavorativa mediante "distruggi documenti".

13. Restituzione degli strumenti ICT

A seguito della cessazione del rapporto lavorativo ovvero al venir meno dei presupposti per l'utilizzo degli strumenti di lavoro, l'Utente è tenuto alla restituzione degli stessi.

Senza l'autorizzazione del Titolare è fatto divieto all'Utente di formattare, alterare, manomettere o distruggere gli strumenti di lavoro assegnati o rendere inintelligibili i dati ivi contenuti.

14. Sorveglianza e controlli difensivi

Il Titolare si riserva la facoltà di effettuare controlli per tutelare la sicurezza dei trattamenti effettuati mediante strumenti informatici nonché la riservatezza, l'integrità e la disponibilità dei dati trattati ed evitare la commissione di illeciti ovvero per esigenze di carattere difensivo anche preventivo, verificare la funzionalità del sistema e degli strumenti informatici.

I controlli avranno natura generale cui potranno seguire eventuali controlli mirati nel caso in cui vengano rilevate anomalie persistenti o minacce alla sicurezza.

Nel caso in cui, dall'analisi dei dati aggregati, vengano rilevate anomalie tali da minare la sicurezza dei dati, potranno essere eseguiti richiami di natura generale nei confronti delle aree o dei reparti in cui tali anomalie sono state riscontrate, con indicazione che, nel caso in cui tali anomalie perdurassero, potranno essere eseguiti ulteriori controlli specifici e maggiormente approfonditi.

Tali controlli generali non avranno natura continuativa, ma verranno attuati saltuariamente e unicamente per scopi difensivi, al fine di garantire adeguata tutela alle informazioni e ai dati. Per tali controlli il Titolare potrà avvalersi di soggetti esterni.

Si precisa che il Titolare non adotta apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori (ex art. 4, comma 1, legge n. 300/1970, c.d. Statuto dei lavoratori), tra cui sono certamente ricomprese le strumentazioni hardware e software mirate al controllo dell'utente né adotta sistemi che determinano interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale e/o privata.

15. Provvedimenti sanzionatori

Il presente Disciplinare risulta correttamente portato a conoscenza di Utenti assegnatari e/o utilizzatori di risorse informatiche del Titolare.

Tutti i lavoratori sono tenuti al rispetto del presente Disciplinare. In caso di inosservanza, il Titolare potrà adottare provvedimenti di natura disciplinare nonché altre sanzioni previste dal CCNL di settore, cui si rimanda per ogni specifica, nonché procedere con le azioni civili e penali che ne dovessero scaturire.

Aggiornamenti e revisione

In virtù dell'evoluzione normativa e tecnologica, il presente Disciplinare potrà essere oggetto di aggiornamento e revisione. Ogni modifica o integrazione verrà portata a conoscenza degli Utenti, così da fornire le nuove istruzioni circa l'utilizzo degli strumenti di lavoro.