Istituto Istruzione Superiore
don Milani
Rovereto

DISCIPLINARE PER L'UTILIZZO DEGLI STRUMENTI ELETTRONICI

INDICE

1. STATO DEL DOCUMENTO

Di seguito viene riportata una tabella dove è indicato lo stato del documento con indicazione della prima emissione e delle varie revisioni del documento stesso.

N° revisione	Data documento	Motivo
00	12.07.2019	*Emissione del documento*

2. SEZIONE I – AMBITO GENERALE

2.1. DEFINIZIONI

2.2. PREMESSA

Le informazioni che vengono gestite a livello possono essere considerate, ai sensi del *regolamento europeo 679/2016* "**dati personali**", quando riguardano dati di persone fisiche e, per la loro gestione (Trattamento), sia cartacea che digitale, è essenziale che IL Titolare adotti una serie di misure adeguate ed idonee previste dalle norme.

Altre informazioni, pur non essendo "dati personali" ai sensi di legge, sono comunque "**informazioni riservate**", ovvero informazioni tecniche, commerciali, contrattuali, di business o di altro genere per le quali l Titolare deve garantirne la riservatezza, o per accordo di non divulgazione (non - disclosure agreement - d'ora in poi anche NDA), o per una più ampia tutela del patrimonio aziendale.

Ai fini di questo Disciplinare si specifica, pertanto, che con il termine "**dati**" si vuole identificare l'insieme più ampio di informazioni di cui un dipendente o un collaboratore può venire a conoscenza e di cui deve assicurare la riservatezza e la segretezza e non solo i "dati personali" intesi a norma di legge.

In linea generale, ogni dato di cui il lavoratore viene a conoscenza, nell'ambito della propria attività lavorativa, è riservato e per tal motivo non deve essere comunicato o diffuso a nessuno (anche una volta interrotto il rapporto lavorativo con l'organizzazione stessa o qualora parte delle informazioni siano di pubblico dominio) salvo specifica autorizzazione esplicita del Titolare del trattamento.

Ciò deve avvenire anche tra colleghi, oppure tra dipendenti e collaboratori esterni, limitandosi solo a quei casi che si rendono necessari per espletare l'attività lavorativa richiesta.

La crescente diffusione delle nuove tecnologie informatiche ed in particolare l'accesso alla rete Internet dal computer aziendale espone l'azienda a possibili rischi di un coinvolgimento di rilevanza sia civile, sia penale, sia amministrativa, creando problemi alla sicurezza e all'immagine della stessa.

Premesso che i comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, tra i quali rientrano l'utilizzo delle risorse informatiche e telematiche, devono sempre ispirarsi al principio di diligenza e correttezza, l'azienda ha adottato il presente Disciplinare Interno per evitare che comportamenti non conformi a quanto stabilito possano innescare problemi o minacce alla sicurezza dei dati o delle attrezzature aziendali.

Il presente Disciplinare Interno si applica ai lavoratori che si trovano ad operare con dati del Titolare. Una gestione dei dati cartacei, un uso dei computer e di altri dispositivi elettronici (di seguito dispositivi) nonché dei servizi di Internet e della posta elettronica difforme dalle regole contenute nel presente Disciplinare potrebbe esporre l'organizzazione ad aumentare la minaccia di accessi non autorizzati ai dati e/o al sistema informatico aziendale, furti o divulgazioni di informazioni riservate nonché furti o danneggiamenti del sistema informatico e/o malfunzionamenti in generale dell'intero

sistema informatico. Le informazioni contenute nel presente Disciplinare vengono rilasciate anche ai sensi del **Regolamento (UE) n. 2016/679** e costituiscono, quindi, parte integrante dell'informativa rilasciata ai soggetti autorizzati.

2.3. ESCLUSIONE ALL'USO DEGLI STRUMENTI INFORMATICI

All'inizio del rapporto lavorativo o di consulenza, il Titolare valuta la presenza dei presupposti per l'autorizzazione all'uso dei vari dispositivi aziendali, di Internet e della posta elettronica da parte degli Incaricati per poi, successivamente, valutarne la permanenza.

È fatto esplicito divieto ai soggetti non autorizzati di accedere alla strumentazione informatica aziendale.

I casi di esclusione possono riguardare:

1. l'utilizzo del computer o di altri dispositivi;
2. l'utilizzo della posta elettronica;
3. l'accesso a Internet.

Le eventuali esclusioni sono strettamente connesse al principio della natura aziendale e lavorativa degli strumenti informatici nonché al principio di necessità di cui al Regolamento Privacy.

Più specificatamente, solo i soggetti designati, per effettivo e concreto bisogno, hanno diritto all'utilizzo degli strumenti e ai relativi accessi.

I casi in cui le esclusioni dovranno risultare operative in forza di tali motivazioni verranno comunicati individualmente e potranno riguardare o tutti i casi sopra descritti, o alcuni di essi.

Si informa che tali esclusioni sono divenute necessarie alla luce del Provvedimento del Garante 1° marzo 2007 che indica, a titolo cautelativo e preventivo, un minor utilizzo degli strumenti informatici visti i pericoli e le minacce indicate in questo documento.

2.4. TITOLARITÀ DEI DISPOSITIVI E DEI DATI

Il Titolare e proprietario esclusivo dei dispositivi messi a disposizione dei singoli soggetti designati soli fini dell'attività lavorativa, di tutte le informazioni, delle registrazioni e dei dati contenuti e/o trattati mediante i propri dispositivi digitali o archiviati in modo cartaceo nei propri locali.

L'incaricato non può presumere o ritenere che le informazioni, le registrazioni ed i dati da lui trattati o memorizzati nei dispositivi aziendali (inclusi i messaggi di posta elettronica e/o chat inviati o ricevuti, i file di immagini, i file di filmati o altre tipologie di file) siano privati o personali, né può presumere che dati cartacei in suo possesso possano essere da lui copiati, comunicati o diffusi senza l'autorizzazione del Titolare.

2.5. FINALITÀ NELL'UTILIZZO DEI DISPOSITIVI

I dispositivi assegnati sono uno strumento lavorativo nelle disponibilità dell'Incaricato esclusivamente per un fine di carattere lavorativo. Ciò presuppone che non devono essere utilizzati per finalità private e diverse da quelle aziendali, se non eccezionalmente e nei limiti evidenziati dal presente Disciplinare.

Qualsiasi eventuale tolleranza da parte del Titolare, apparente o effettiva, non potrà, comunque, legittimare comportamenti contrari alle istruzioni contenute nel presente documento.

2.6. RESTITUZIONE DEI DISPOSITIVI

Quando vi è una cessazione del rapporto lavorativo (o di consulenza) soggetto designato con il Titolare o del venir meno, ad insindacabile giudizio del Titolare stesso, della permanenza dei presupposti per l'utilizzo dei dispositivi aziendali, gli Incaricati hanno i seguenti obblighi:

1. restituire immediatamente i dispositivi in uso;
2. non formattare o alterare o manomettere o distruggere i dispositivi assegnati o rendere inintelligibili i dati in essi contenuti tramite qualsiasi processo.

2.7. RESTITUZIONE DEI DATI CARTACEI

Quando vi è una cessazione del rapporto lavorativo (o di consulenza) del soggetto incaricato con l'organizzazione o del venir meno, ad insindacabile giudizio dell'azienda, della permanenza dei presupposti per l'utilizzo di dati cartacei aziendali, gli Incaricati hanno i seguenti obblighi:

1. restituire immediatamente i dati cartacei in loro possesso;
2. non alterare o manomettere o distruggere i dati cartacei assegnati o renderli inintelligibili tramite qualsiasi processo.

3. SEZIONE II – PASSWORD

3.1. LE PASSWORD

Le password rappresentano un metodo di autenticazione assegnato dal Titolare per garantire l'accesso protetto ad uno strumento hardware oppure ad un applicativo software.

La prima caratteristica di una password è la segretezza in quanto non deve essere svelata ad altri soggetti. La divulgazione delle proprie password o la trascuratezza nella loro conservazione può essere fonte di gravi danni al proprio lavoro, a quello dei colleghi e dell'azienda nel suo complesso.

È importante ricordare che, nel tempo, anche la password più sicura perde la sua segretezza. Per tal motivo è necessario cambiarle con una certa frequenza.

Il Titolare ha attivato alcuni meccanismi che aiutano e supportano gli Incaricati in una corretta gestione delle password, in particolare, per quanto riguarda le password di accesso al Dominio (ove previsto): è, infatti, in funzione un sistema automatico di richiesta di aggiornamento delle stesse impostato dall'azienda secondo il livello di sicurezza richiesto dall'azienda stessa e, comunque, in linea con quanto richiesto dalla normativa privacy.

Altra buona norma è quella di non memorizzare la password su supporti facilmente intercettabili da altre persone. Il miglior luogo in cui conservare una password è la propria memoria.

Le password che non vengono utilizzate da parte dei soggetti autorizzati per un periodo superiore ai sei mesi verranno disattivate.

In qualsiasi momento il Titolare si riserva il diritto di revocare all'Incaricato il permesso di accedere ad un sistema hardware o software a cui era precedentemente autorizzato, rimuovendo user id o modificando/cancellando la password ad esso associata.

3.2. REGOLE PER LA CORRETTA GESTIONE DELLE PASSWORD

L'Incaricato, da parte sua, deve rispettare le seguenti regole per una corretta e sicura gestione delle proprie password:

1. le password sono assolutamente personali e non vanno mai comunicate ad altri;
2. occorre cambiare immediatamente una password nel momento in cui diventa poco "sicura";
3. le password devono essere lunghe almeno 8 caratteri e devono contenere anche lettere maiuscole, caratteri speciali1 e numeri;
4. 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);
5. le password devono essere sostituite almeno nei tempi indicati dalla normativa, a prescindere dall'esistenza di un sistema automatico di richiesta di aggiornamento password;
6. le password devono essere digitate in assenza di altri soggetti, i quali potrebbero vederne la digitazione sulla tastiera, anche se collaboratori o dipendenti dell'azienda.

In alcuni casi, sono implementati meccanismi che consentono ai soggetti autorizzati 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 per alcuni minuti. In caso di necessità contattare il Titolare.

1 Per caratteri speciali si intendono, per esempio, i seguenti: { } [ ] , . < > ; : ! " £ $ % & / ( ) = ? ^ \ | ' * - +

3.3. DIVIETO DI USO

Per una corretta gestione delle password, l'organizzazione vieta di utilizzare come propria password:

1. nome, cognome e loro parti;
2. lo username assegnato;
3. un indirizzo di posta elettronica (e-mail);
4. parole comuni (in inglese e in italiano);
5. date, mesi dell'anno e giorni della settimana, anche in lingua straniera;
6. parole banali e/o di facile intuizione, ad es. pippo, security e palindromi (simmetria: radar);
7. ripetizioni di sequenze di caratteri (es. abcabcabc);
8. una password già usata in precedenza.

3.4. ALCUNI ESEMPI DI PASSWORD NON AMMESSE

La password ideale deve essere complessa, senza alcun riferimento alla persona che la utilizza, ma facile da ricordare. Una possibile tecnica è usare sequenze di caratteri prive di senso evidente, ma con singoli caratteri che formano una frase facile da memorizzare (es.: "NIMzz5DICmm!", Nel Mezzo Del Cammin, più il carattere 5 e il punto esclamativo). Alcuni esempi di password assolutamente da evitare:

1. se username = "mariorossi", password = "mario", o ancora peggio, password = "mariorossi";
2. il nome della moglie/marito, fidanzato/a, figli, ecc. anche a rovescio;
3. la propria data di nascita, quella del coniuge, ecc.;
4. targa della propria auto;
5. numero di telefono proprio, del coniuge, ecc.;
6. parole comuni tipo "Kilimangiaro", "Password", "Qwerty", "12345678" (troppo facili);
7. qualsiasi parola del vocabolario (di qualsiasi lingua diffusa, come inglese, italiano, ecc.).

3.5. LA PASSWORD NEI SISTEMI

Ogni Incaricato può modificare la propria password di accesso a qualsiasi sistema aziendale in modo autonomo, qualora il sistema in questione metta a disposizione degli Utenti una funzionalità di questo tipo (Change password), oppure facendone richiesta al Titolare. La password può essere sostituita dal Titolare, anche qualora l'Utente l'abbia dimenticata.

3.6. AUDIT DELLE PASSWORD

Nell'ambito delle attività riguardanti la tutela della sicurezza della infrastruttura tecnologica, il Titolare potrebbe effettuare analisi periodiche sulle password degli Incaricati al fine di verificarne la solidità, le policy di gestione e la durata, informandone preventivamente gli Incaricati stessi.

Nel caso in cui l'audit abbia, tra gli esiti possibili, la decodifica della password, questa viene bloccata e al soggetto designato, viene richiesto di cambiarla.

4. SEZIONE III – OPERAZIONI A PROTEZIONE DELLA POSTAZIONE DI LAVORO

In questa sezione vengono trattate le operazioni a carico del soggetto designato e il quadro di riferimento generale per l'esecuzione delle stesse a protezione della propria postazione di lavoro, nel rispetto della sicurezza e dell'integrità del patrimonio aziendale.

4.1. LOGIN E LOGOUT

Il "Login" è l'operazione con la quale l'Incaricato si connette al sistema informativo aziendale o ad una parte di esso, inserendo il proprio Username e Password (ossia l'Account), aprendo così 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.
In questi casi, sebbene sia preferibile che ogni utente abbia un suo specifico user name e password, il titolare potrà assegnare un univoco user name e password per gruppi di soggetti autorizzati per l'accesso alla macchina fisica, mentre rimarranno separati ed univoci per l'accesso agli applicativi che contengono dati.

Il "Logout" è l'operazione con cui viene chiusa la sessione di lavoro. Al termine della giornata lavorativa, tutte le applicazioni devono essere chiuse secondo le regole previste dall'applicazione stessa in quanto la non corretta chiusura può provocare una perdita di dati o l'accesso agli stessi da parte di persone non autorizzate.
Il "blocco del computer" è l'operazione con cui viene impedito l'accesso alla sessione di lavoro (tastiera e schermo disattivati) senza chiuderla.

4.2. OBBLIGHI

L'utilizzo dei dispositivi fisici e la gestione dei dati ivi contenuti devono svolgersi nel rispetto della sicurezza e dell'integrità del patrimonio dati aziendale.
L'incaricato deve quindi eseguire le operazioni seguenti:

1. se si allontana dalla propria postazione dovrà mettere in protezione il suo dispositivi per evitare che persone non autorizzate abbiano accesso ai dati protetti;
2. bloccare il dispositivo prima delle pause e, più in generale, ogni qual volta si allontanerà dalla propria postazione;
3. chiudere la sessione (Logout) a fine giornata;
4. spegnere il PC dopo il Logout;
5. controllare sempre che non vi siano persone non autorizzate alle sue spalle che possano prendere visione delle schermate del dispositivo.

5. SEZIONE IV - USO DEL PERSONAL COMPUTER AZIENDALE

5.1. MODALITÀ D'USO DEL COMPUTER AZIENDALE

Il sistema informatico aziendale è costituito da un insieme di unità server centrali e macchine client connessi ad una rete locale (LAN), che utilizzano diversi sistemi operativi e applicativi.

I file creati, elaborati o modificati sul computer assegnato devono essere poi sempre salvati a fine giornata sul sistema di repository documentale centralizzato. Non vengono effettuati backup dei dati memorizzati in locale.

5.2. CORRETTO UTILIZZO DEL COMPUTER AZIENDALE

Il computer consegnato all'incaricato 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, con un conseguente aumento dei costi di manutenzione e, soprattutto, di minacce alla sicurezza.

L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. Per necessità aziendali, gli amministratori di sistema utilizzando la propria login con privilegi di amministratore e la password dell'amministratore, potranno accedere, con le regole indicate nel presente documento, sia alle memorie di massa locali di rete (repository e backup) che ai server aziendali nonché, previa comunicazione al dipendente, accedere al computer, anche in remoto. In particolare, l'Incaricato deve adottare le seguenti misure:

1. utilizzare solo ed esclusivamente le aree di memoria della rete aziendale con la possibilità di creare e registrare file e software o archivi dati, senza pertanto creare altri file fuori dalle unità di rete;
2. spegnere il computer, o curarsi di effettuare il logout, ogni sera prima di lasciare gli uffici o in caso di assenze prolungate;
3. mantenere sul computer esclusivamente i dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori), disposti dall'organizzazione;
4. non dare accesso al proprio computer ad altri utenti, a meno che siano Incaricati con cui condividono l'utilizzo dello stesso Pc o a meno di necessità stringenti e sotto il proprio costante controllo.

5.3. DIVIETI ESPRESSI SULL'UTILIZZO DEL COMPUTER

All'incaricato è fatto divieto:

1. gestire e memorizzare (anche temporaneamente) o trattare file, documenti e/o informazioni personali o comunque non afferenti alle attività lavorative nella rete, nel disco fisso o in altre memorie di massa aziendali e negli strumenti informatici aziendali in genere;
2. modificare le configurazioni già impostate sul personal computer;
3. utilizzare programmi e/o sistemi di criptazione senza la preventiva autorizzazione scritta dell'Azienda;
4. installare software di cui il Titolare non possieda la licenza, né installare alcuna versione diversa rispetto alle applicazioni o al sistema operativo presenti sul personal computer consegnato, senza l'espressa autorizzazione del Titolare, né ancora fare copia del software installato al fine di farne un uso personale;

5. caricare sul disco fisso del computer o nel server documenti, giochi, file musicali o audiovisivi o immagini diversi da quelli necessari allo svolgimento delle mansioni affidate;
6. aggiungere o collegare dispositivi hardware (ad esempio hard disk, driver, PCMCIA, ecc.) o periferiche (telecamere, macchine fotografiche, smartphone, chiavi USB ecc.) diversi da quelli consegnati, senza l'autorizzazione espressa del Titolare;
7. creare o diffondere, intenzionalmente o per negligenza, programmi idonei a danneggiare il sistema informatico del Titolare, quali per esempio virus, trojan horses ecc.;
8. accedere, rivelare o utilizzare informazioni non autorizzate o comunque non necessarie per le mansioni svolte;
9. effettuare in proprio attività manutentive;
10. permettere attività manutentive da parte dei soggetti non espressamente autorizzati del Titolare.

5.4. ANTIVIRUS

I virus possono essere trasmessi tramite scambio di file via Internet, via mail, per mezzo di supporti removibili, file sharing, chat, via mail ecc.

Il Titolare 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'incaricato deve controllare il corretto funzionamento e aggiornamento del sistema antivirus installato sul proprio computer, e, in particolare, deve rispettare le regole seguenti:

1. comunicare al Titolare ogni anomalia o malfunzionamento del sistema antivirus;
2. comunicare al Titolare eventuali segnalazioni di presenza di virus o file sospetti.

Inoltre, all'incaricato:

1. è vietato accedere alla rete aziendale senza servizio antivirus attivo e aggiornato sulla propria postazione;
2. è vietato ostacolare l'azione dell'antivirus aziendale;
3. è vietato disattivare l'antivirus senza autorizzazione espressa anche e soprattutto nel caso sia richiesto per l'installazione di software sul computer;
4. è vietato aprire allegati di mail provenienti da mittenti sconosciuti o di dubbia provenienza o allegati di mail di persone conosciute ma con testi inspiegabili o in qualche modo strani;
5. è vietato contattare i sistemi informativi prima di procedere a qualsiasi attività potenzialmente in conflitto con quanto sopra.

6. SEZIONE V – INTERNET

6.1. INTERNET È UNO STRUMENTO DI LAVORO

La connessione alla rete Internet dal dispositivo avuto in dotazione è ammessa esclusivamente per motivi attinenti allo svolgimento dell'attività lavorativa. L'utilizzo per scopi personali è permesso con moderazione (e solo durante le pause previste), con gli accorgimenti di cui al presente documento. In particolare, si vieta l'utilizzo dei social network, se non espressamente autorizzati.

6.2. MISURE PREVENTIVE PER RIDURRE NAVIGAZIONI ILLECITE

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

6.3. DIVIETI ESPRESSI CONCERNENTI INTERNET

1. è vietata la navigazione nei siti che possono rivelare le opinioni politiche religiose, sindacali e di salute dell'Incaricato poiché potenzialmente idonea a rivelare dati particolari ai sensi del Regolamento Privacy;
2. è fatto divieto di 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, degli handicap;
3. è vietato all'Incaricato lo scarico di software (anche gratuito) prelevato da siti Internet;
4. è tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dal Titolare e con il rispetto delle normali procedure di acquisto;
5. è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
6. è vietata la partecipazione a forum non professionali, l'utilizzo di chat line, di bacheche elettroniche o partecipare a gruppi di discussione o lasciare commenti ad articoli o iscriversi a mailing list spendendo il marchio o la denominazione del Titolare, salvo specifica autorizzazione del Titolare stessa;
7. è vietata 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. è vietato al soggetto designato di promuovere utile o guadagno personale attraverso l'uso di Internet o della posta elettronica aziendale;
9. è vietato accedere dall'esterno alla rete interna del Titolare, salvo con le specifiche procedure previste dall'azienda stesso;
10. è vietato, infine, creare siti web personali sui sistemi del Titolare nonché acquistare beni o servizi su Internet a meno che l'articolo acquistato non sia stato approvato a titolo di spesa professionale.

Ogni eventuale navigazione di questo tipo, comportando un illegittimo utilizzo di Internet, nonché un possibile illecito trattamento di dati personali e sensibili è posta sotto la personale responsabilità dell'Incaricato inadempiente.

6.4. DIVIETI DI SABOTAGGIO

È vietato accedere ad alcuni siti internet mediante azioni inibenti dei filtri, sabotando, superando o tentando di superare o disabilitando i sistemi adottati dall'azienda per bloccare accessi non conformi all'attività lavorativa. In ogni caso è vietato utilizzare siti o altri strumenti che realizzino tale fine.

6.5. 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. 248).

In particolare, è vietato il download di materiale soggetto a copyright (testi, immagini, musica, filmati, file in genere) se non espressamente autorizzato dall'organizzazione.

7. SEZIONE VI – POSTA ELETTRONICA

7.1. LA POSTA ELETTRONICA È UNO STRUMENTO DI LAVORO

L'utilizzo della posta elettronica aziendale è connesso allo svolgimento dell'attività lavorativa. L'uso per motivi personali deve essere moderato ed è tollerato esclusivamente ai sensi dell'articolo seguente. Gli Incaricati possono avere in utilizzo indirizzi nominativi di posta elettronica.

Le caselle e-mail possono meglio essere assegnate con natura impersonale (tipo info, amministrazione, fornitori, direttore, direttore sanitario, consulenza, ...) proprio per evitare ulteriormente che il destinatario delle mail possa considerare l'indirizzo assegnato al dipendente "privato", ai sensi dei suggerimenti del Garante a tal proposito.

Gli Incaricati assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

7.2. MISURE PREVENTIVE PER RIDURRE UTILIZZI ILLECITI DELLA POSTA ELETTRONICA

Il Titolare è consapevole della possibilità di un limitato utilizzo personale della posta elettronica da parte degli Incaricati e allo scopo prevede le seguenti misure:

1. in caso di ricezione sulla e-mail aziendale di posta personale si avverte di cancellare immediatamente ogni messaggio al fine di evitare ogni eventuale e possibile back up dei dati;
2. avvisare l'organizzazione quando alla propria posta personale siano allegati file eseguibili e/o di natura incomprensibile o non conosciuta.

7.3. DIVIETI ESPRESSI

1. è vietato utilizzare l'indirizzo di posta elettronica contenente il dominio del Titolare per iscriversi in qualsivoglia sito per motivi non attinenti all'attività lavorativa, senza espressa autorizzazione scritta del Titolare, nonché utilizzare il dominio del Titolare per scopi personali;
2. è vietato redigere messaggi di posta elettronica utilizzando l'indirizzo aziendale, diretti a destinatari esterni del Titolare, senza utilizzare il seguente disclaimer o uno equivalente:
   "In conformità a quanto disposto dal Regolamento Europeo 2016/679, questa comunicazione e ogni eventuale file allegato sono confidenziali e destinati all'uso esclusivo del destinatario. Se avete ricevuto questo messaggio per errore Vi preghiamo di comunicarlo al mittente e distruggere quanto ricevuto. Il mittente, tenuto conto del mezzo utilizzato, non si assume alcuna responsabilità in ordine alla segretezza e riservatezza delle informazioni contenute nella presente comunicazione via e-mail. Per l'informativa completa si rinvia al sito www.domir.it";
3. è vietato 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. è vietato trasmettere messaggi a gruppi numerosi di persone (es. a tutto un ufficio o ad un'intera divisione) senza l'autorizzazione necessaria;
5. è vietato sollecitare donazioni di beneficenza, propaganda elettorale o altre voci non legate al lavoro;

6. è vietato utilizzare il servizio di posta elettronica per trasmettere a soggetti esterni del Titolare informazioni riservate o comunque documenti aziendali, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte;
7. è vietato utilizzare la posta elettronica per messaggi con allegati di grandi dimensioni.

7.4. POSTA ELETTRONICA IN CASO DI ASSENZE PROGRAMMATE ED ASSENZE NON PROGRAMMATE

Nel caso di assenza prolungata sarebbe buona norma attivare il servizio di risposta automatica (Autoreply).
In alternativa e in tutti i casi in cui sia necessario un presidio della casella di e-mail per ragioni di operatività aziendale, l'Incaricato deve nominare un collega fiduciario con lettera scritta che in caso di assenza inoltri i file necessari a chi ne abbia urgenza.
Qualora l'Incaricato non abbia provveduto ad individuare un collega fiduciario o questi sia assente o irreperibile, il Titolare, mediante personale appositamente incaricato, potrà verificare il contenuto dei messaggi di posta elettronica dell'incaricato, informandone l'incaricato stesso e redigendo apposito verbale.

7.5. UTILIZZO ILLECITO DI POSTA ELETTRONICA

1. È vietato 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;
2. è vietato inviare messaggi di posta elettronica, anche all'interno della rete aziendale, che abbiano contenuti contrari a norme di legge e a norme di tutela dell'ordine pubblico, rilevanti ai fini della realizzazione di una fattispecie di reato, o che siano in qualche modo discriminatori della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap;
3. qualora l'Incaricato riceva messaggi aventi tale contenuto, è tenuto a cancellarli immediatamente e a darne comunicazione all'organizzazione.

8. SEZIONE VII – USO DI ALTRI DISPOSITIVI (PERSONAL COMPUTER PORTATILE, TABLET, CELLULARE, SMARTPHONE E DI ALTRI DISPOSITIVI ELETTRONICI)

8.1. L'UTILIZZO DEL NOTEBOOK, TABLET O SMARTPHONE

Il Titolare può concedere in uso il computer portatile, il tablet e il cellulare (di seguito generalizzati in "dispositivi mobile") ai soggetti autorizzati che necessitano di disporre di archivi elettronici, supporti di automazione e/o di connessione alla rete del Titolare durante gli spostamenti.

L'Incaricato è responsabile dei dispositivi mobili assegnatigli dall'organizzazione e ha il compito di custodirli con diligenza.

Ai dispositivi mobili si applicano le regole di utilizzo previste per i computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna. In particolare, i file creati o modificati sui dispositivi mobili devono essere trasferiti sulle memorie di massa aziendali al primo rientro in ufficio e cancellati in modo definitivo dai dispositivi mobili (Wiping). Sui dispositivi mobili è vietato installare applicazioni (anche gratuite) se non espressamente autorizzate dal Titolare. I dispositivi mobili utilizzati all'esterno (convegni, visite in azienda, ecc), in caso di allontanamento, devono essere custoditi in un luogo protetto. In caso di perdita o furto deve seguire la denuncia alle autorità competenti e avvisare immediatamente il Titolare che provvederà – se del caso – ad occuparsi delle procedure connesse alla privacy. Anche di giorno, durante l'orario di lavoro, l'Incaricato non deve lasciare incustoditi i dispositivi mobili.

All'Incaricato è vietato lasciare i dispositivi mobili incustoditi e a vista dentro l'auto, in una stanza d'albergo, nell'atrio dell'albergo o nelle sale d'attesa delle stazioni ferroviarie e aeroportuali.

I dispositivi mobili che permettono l'attivazione di una procedura di protezione (PIN) devono sempre essere abilitabili con la digitazione del PIN.

Laddove il dispositivo mobile sia accompagnato da un'utenza, l'Incaricato è chiamato ad informarsi preventivamente dei vincoli ad essa associati (es. numero minuti massimo, totale gigabyte dati, ...) e a rispettarli. Nel caso questi ultimi richiedessero requirements differenti, l'Incaricato deve informare tempestivamente e preventivamente il Titolare.

In relazione alle utenze mobili, salvo autorizzazione del Titolare, è espressamente vietato ogni utilizzo all'estero e anche in caso di autorizzazione del Titolare, gli utilizzi all'estero devono essere preventivamente comunicati all'organizzazione per permettere l'attivazione di opportuni contratti di copertura con l'operatore mobile di riferimento.

8.2. MEMORIE ESTERNE (CHIAVI USB E SIMILARI, HARD DISK, CD-ROM, DVD, ECC.)

Agli Incaricati può essere assegnata una memoria esterna (quale una chiave USB, un hard disk esterno, una memory card) su cui copiare temporaneamente dei dati per un facile trasporto, o altri usi (es. macchine fotografiche con memory card, videocamere con dvd).

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.

8.3. DISPOSITIVI PERSONALI

Ai dipendenti non è permesso svolgere la loro attività su PC fissi, portatili, dispositivi personali ad eccezione dell'utilizzo della posta elettronica aziendale, quando espressamente autorizzati dall'azienda. In questo caso è necessario che il dispositivio abbia password di sicurezza stringenti approvate dal Titolare e l'eventuale furto o smarrimento deve essere immediatamente segnalato anche all'azienda per eventuali provvedimenti di sicurezza.

Al collaboratore è vietato l'utilizzo di memorie esterne personali (quali chiavi USB, memory card, cdrom, DVD, macchine fotografiche, videocamere, tablet).

I consulenti e collaboratori esterni possono utilizzare i propri dispositivi personali per memorizzare dati del Titolare solo se espressamente autorizzati dal Titolare stesso e assumendone formalmente e personalmente l'intera responsabilità del trattamento.

Tali dispositivi dovranno essere preventivamente valutati dall'azienda, per la verifica della sussistenza di misure adeguate ed idonee di sicurezza.

8.4. UTILIZZO DEL CELLULARE/SMARTPHONE PERSONALE

Durante l'orario di lavoro, comprese le eventuali pause, agli Incaricati è permesso utilizzare il telefono cellulare personale ma solo per comunicazioni di emergenza o strettamente collegate all'ambito lavorativo. Nel caso di trasferte lavorative all'esterno degli uffici del Titolare, il telefono personale può rimanere acceso, anche per facilitare la comunicazione con l'organizzazione stessa ove fosse necessario. Nonostante ciò, si invita, comunque, a non utilizzarlo per fini personali, in modo particolare alla presenza di clienti o fornitori.

I consulenti e collaboratori esterni possono utilizzare i propri cellulari/smartphone per memorizzare dati del Titolare solo se espressamente autorizzati e assumendone formalmente e personalmente l'intera responsabilità del trattamento.

Tali cellulari/smartphone dovranno essere preventivamente valutati dal Titolare, per la verifica della sussistenza di misure adeguate ed idonee di sicurezza.

8.5. DISTRUZIONE DEI DISPOSITIVI

Ogni dispositivi 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 al Titolare che provvederà a distruggerli o a ricondizionarli seguendo le norme di legge in vigore al momento.

In particolare, il Titolare provvederà a cancellare o a rendere inintelligibili i dati negli stessi memorizzati.

9. SEZIONE VIII – SISTEMI IN CLOUD

9.1. CLOUD COMPUTING

In campo informatico, con il termine inglese cloud computing (in italiano nuvola informatica) si indica un sistema 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.

Le risorse non vengono pienamente configurate e messe in opera dal fornitore apposta per l'utente, ma gli sono assegnate grazie a procedure automatizzate, a partire da un insieme di risorse condivise con altri utenti lasciando all'utente parte dell'onere della configurazione. Quando l'utente rilascia la risorsa, essa viene similmente riconfigurata nello stato iniziale e rimessa a disposizione nel pool condiviso delle risorse, con altrettanta velocità ed economia per il fornitore.

Utilizzare un servizio di cloud computing per memorizzare dati personali o sensibili, espone l'azienda a potenziali problemi di violazione della privacy. I dati personali vengono memorizzati nei server farms di aziende che spesso risiedono in uno stato diverso da quello dell'azienda. Il cloud provider, in caso di comportamento scorretto o malevolo, potrebbe accedere ai dati personali per eseguire ricerche di mercato e profilazione degli utenti.

Con i collegamenti wireless, il rischio sicurezza aumenta e si è maggiormente esposti ai casi di pirateria informatica a causa della minore sicurezza offerta dalle reti senza fili. In presenza di atti illegali, come appropriazione indebita o illegale di dati personali, il danno potrebbe essere molto grave per l'azienda, con difficoltà di raggiungere soluzioni giuridiche e/o rimborsi se il fornitore risiede in uno stato diverso da paese dell'utente.

Nel caso di industrie o aziende, tutti i dati memorizzati nelle memorie esterne sono seriamente esposti a eventuali casi di spionaggio industriale.

9.2. UTILIZZO DI SISTEMI CLOUD

È vietato agli Incaricati l'utilizzo di sistemi cloud non espressamente approvati dall'azienda. Per essere approvati, devono rispondere ad almeno i seguenti requisiti:

- essere sistemi cloud esclusivi e non condivisi;
- essere sistemi cloud posizionati fisicamente in Europa;
- l'azienda che fornisce il sistema in cloud deve essere preventivamente nominata Responsabile del Trattamento dei dati da parte del Titolare;
- l'azienda che fornisce il sistema in cloud deve comunicare all'azienda, almeno una volta all'anno, i nominativi degli amministratori di sistema utilizzati;
- dovranno essere verificate tutte le indicazioni e prescrizioni previste dal Garante della Privacy nei suoi provvedimenti sugli Amministratori di Sistema e sul cloud.

10. CLEAR DESK POLICY

Gli Incaricati sono responsabili del controllo e della custodia degli atti e dei documenti contenenti dati personali per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento.

I soggetti autorizzati sono invitati dal Titolare ad adottare una "politica della scrivania pulita". Ovvero si richiede agli Incaricati di trattare dati cartacei solo se necessario, privilegiando, ove possibile, l'utilizzo degli strumenti digitali messi a disposizione dal Titolare.

I principali benefici di una politica della scrivania pulita sono:

1) una buona impressione a clienti e fornitori che visitano la nostra organizzazione;
2) la riduzione della possibilità che informazioni confidenziali possano essere viste da persone non abilitate a conoscerle;
3) la riduzione che documenti confidenziali possano essere sottratti all'organizzazione.

In particolare, si invita a non lasciare in vista dati cartacei sulla propria scrivania quando ci si allontana dalla stessa oppure quando è previsto un incontro con un soggetto non abilitato alla conoscenza dei dati in essi contenuti.

Prima di lasciare la propria postazione (per esempio per la pausa pranzo o per una riunione) sarà cura degli Incaricati riporre in luogo sicuro (armadio, cassettiera, archivio) i dati cartacei ad esso affidati, affinché gli stessi non possano essere visti da terzi non autorizzati (es. addetti alle pulizie) o da terzi (visitatori) presenti all'interno della struttura aziendale.

A fine giornata deve essere previsto il riordino della scrivania e la corretta archiviazione di tutte le pratiche d'ufficio, in modo da lasciare la scrivania completamente sgombra.

Ove possibile, si invita ad evitare la stampa di documenti digitali, anche ai fini di ridurre l'inquinamento ed il consumo delle risorse in ottica ecologica, effettuando invece la scansione dei documenti cartacei ed archiviarli digitalmente.

È necessario rimuovere immediatamente ogni foglio stampato da una stampante o da un'apparecchiatura fax, per evitare che siano prelevati o visionati da soggetti non autorizzati.

Ove possibile, è buona norma eliminare i documenti cartacei attraverso apparecchiature trita documenti.

Per favorire il rispetto degli obblighi di confidenzialità, vengono emanate delle linee guida che aiutino i dipendenti a far sì che sia assicurato che i dati personali dei utenti e degli altri lavoratori ricevano adeguata protezione, in accordo con le disposizioni vigenti in materia di protezione dei dati personali. Tramite tali accorgimenti, inoltre, si vuole evitare l'insorgere sia del rischio di frode, ossia di appropriazione ed utilizzo da parte di esterni di informazioni ritenute sensibili, sia il rischio reputazionale. Pertanto, tutti i dipendenti e collaboratori hanno l'obbligo di:

- non lasciare informazioni sulla scrivania durante la notte: riporre sempre la documentazione sensibile in appositi armadi chiusi a chiave;
- non lasciare documenti nella stampante durante la notte;
- non lasciare documenti incustoditi in prossimità di macchine stampanti/fotocopiatrici/fax o nella sala riunione;
- utilizzare sempre il distruggi-documenti in caso di non utilità di copie cartacee;

- non lasciare il personal computer incustodito quando si sta lavorando su documentazione sensibile (utilizzare lo screen saver ctrl+alt+canc);
- utilizzare internet e l'indirizzo di posta elettronica in maniera adeguata all'esclusivo scopo lavorativo;
- non inviare informazioni sensibili ad indirizzi di posta personali;
- non lasciare la password di accesso del proprio computer incustodita;
- non lasciare informazioni personali incustodite (carte di credito, indirizzi personali, numeri di telefono personali). In caso di cessazione del rapporto di lavoro/collaborazione, il dipendente/collaboratore ha l'obbligo di riconsegnare tutto il materiale confidenziale o contenente informazioni riservate.

Qualsiasi dipendente che venga sorpreso a violare questa policy potrebbe incorrere in sanzioni disciplinari.

11. SEZIONE X - APPLICAZIONE E CONTROLLO

11.1. IL CONTROLLO

Il Titolare in quanto proprietario degli strumenti informatici, dei dati ivi contenuti e/o trattati, si riserva la facoltà di effettuare i controlli che ritiene opportuni per le seguenti finalità:

1. tutelare la sicurezza e preservare l'integrità degli strumenti informatici e dei dati;
2. evitare la commissione di illeciti o per esigenze di carattere difensivo anche preventivo;
3. verificare la funzionalità del sistema e degli strumenti informatici.

Le attività di controllo potranno avvenire anche con audit e vulnerability assesment del sistema informatico. Per tali controlli il Titolare si riserva di avvalersi di soggetti esterni.

Si precisa, in ogni caso, che il Titolare non adotta "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori" (ex art. 4, primo comma, l. n. 300/1970), tra cui sono certamente comprese le strumentazioni hardware e software mirate al controllo dell'utente.

11.2. MODALITÀ DI VERIFICA

In applicazione del principio di necessità ai sensi del GDPR, il Titolare promuove ogni opportuna misura volta a prevenire il rischio di utilizzi impropri e, comunque, a "minimizzare" l'uso di dati riferibili agli Incaricati e allo scopo ha adottato ogni possibile strumento tecnico, organizzativo e fisico, volto a prevenire trattamenti illeciti sui dati trattati con strumenti informatici. Il Titolare 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 Incaricati avvengono nel rispetto del principio di pertinenza e non eccedenza, con esclusione di registrazioni o verifiche con modalità sistematiche.

Qualora nell'ambito di tali verifiche si dovesse rilevare un evento dannoso, una situazione di pericolo o qualche altra modalità non conforme all'attività lavorativa (es. scarico di file pirata, navigazioni da cui sia derivato il download di virus informatici, ecc.) si effettuerà un avvertimento in modo generalizzato con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

11.3. MODALITÀ DI CONSERVAZIONE

I sistemi software sono stati programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

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

1. Ad esigenze tecniche o di sicurezza del tutto particolari;
2. all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
3. all'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 di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

12. SEZIONE XI – SOGGETTI PREPOSTI DEL TRATTAMENTO, INCARICATI E RESPONSABILI

12.1. INDIVIDUAZIONE DEI SOGGETTI AUTORIZZATI

I soggetti preposti al connesso trattamento dei dati (in particolare, gli Incaricati della manutenzione) sono stati appositamente autorizzati a svolgere solo operazioni strettamente necessarie al perseguimento delle finalità di sicurezza informatica, senza realizzare attività di controllo a distanza, neanche di propria iniziativa.

I soggetti che operano in qualità di amministratori di sistema o le figure analoghe cui siano rimesse operazioni connesse al regolare funzionamento dei sistemi svolgono, invece, un'attività formativa sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni.

13. SEZIONE XII – PROVVEDIMENTI DISCIPLINARI

13.1. CONSEGUENZE DELLE INFRAZIONI DISCIPLINARI

Le infrazioni disciplinari alle norme del presente Disciplinare Interno potranno essere punite, a seconda della gravità delle mancanze, in conformità alle disposizioni di legge e/o del Contratto Collettivo Nazionale del Lavoro applicato, tra cui:

1. il biasimo inflitto verbalmente;
2. lettera di richiamo inflitto per iscritto;
3. multa;
4. la sospensione dalla retribuzione e dal servizio;
5. il licenziamento disciplinare e con le altre conseguenze di ragioni e di legge.

Per i dirigenti valgono le vigenti norme di legge e/o di contrattazione collettiva, fermo restando che, per le violazioni di maggior gravità l'azienda potrà procedere al licenziamento del dirigente autore dell'infrazione.

13.2. MODALITÀ DI ESERCIZIO DEI DIRITTI

Il lavoratore interessato del trattamento dei dati effettuato mediante strumenti informatici ha diritto di accedere ai sensi dell'art. 15 alle informazioni che lo riguardano scrivendo al Titolare del Titolare.

14. SEZIONE XIII – VALIDITA', AGGIORNAMENTO ED AFFISSIONE

14.1. VALIDITÀ

Il presente Disciplinare ha validità a partire dal: 12/07/2019

14.2. AGGIORNAMENTO

Il presente Disciplinare sarà oggetto di aggiornamento ogni volta che se ne ravvisi la necessità, in caso di variazioni tecniche dei sistemi del Titolare o in caso di mutazioni legislative.
Ogni variazione del presente Disciplinare sarà comunicata agli Incaricati.

14.3. AFFISSIONE

Il presente Disciplinare verrà affisso sul sito web istituzionale www.domir.it ai sensi dell'art. 7 della legge 300/70 e del CCNL.

La Dirigente Scolastica
(prof.ssa Daniela Simoncelli)

ISTITUTO DI ISTRUZIONE SUPERIORE "don L. Milani" ROVERETO

Firma del Titolare o Responsabile del trattamento dei dati
La Dirigente Scolastica Prof.ssa Daniela Simoncelli

Data 12/07/2019

Copia del presente documento viene rilasciata al soggetto interessato.