FINPIEMONTE

REGOLAMENTO SULL'UTILIZZO DEGLI STRUMENTI INFORMATICI

Approvato dal Consiglio di Amministrazione in data 19 dicembre 2019

SOMMARIO

1. INTRODUZIONE

Il presente regolamento riporta le disposizioni da osservare per un corretto utilizzo degli strumenti informatici aziendali, in ottemperanza alle esigenze di sicurezza e di protezione sia dei dati personali e a cautela del lavoratore (dipendenti, interinali, stagisti…), sia di quelli aziendali, al fine di non causare danni a seguito di un cattivo utilizzo degli strumenti informatici.

Gli strumenti informatici dati in uso al personale per espletare le attività lavorative sono di proprietà di Finpiemonte S.p.A..

1.1 Scopo, ambito di applicazione e sanzioni

Il presente documento ha diversi scopi fra di loro interconnessi, ovvero:

- illustrare e disciplinare le modalità di utilizzo del sistema informativo interno dell'organizzazione. Per sistema informativo interno, si intende sia la rete interna, sia ogni strumento informatico ad esso collegato (pc, tablet, telefoni, e di ogni altro dispositivo elettronico affidato dall'Organizzazione ai lavoratori e/o collaboratori esterni);
- regolamentare le modalità di fruizione dei servizi che, tramite i sistemi ICT, è possibile ricevere o offrire all'interno e all'esterno dell'organizzazione;
- descrivere la gestione dei dati personali;
- identificare e garantire i diritti dell'interessato in ottemperanza alla legislazione sulla privacy;
- stabilire regole generali sui concetti di sicurezza informatica ed informativa;
- dichiarare lo stato di possesso e proprietà dei dati in gestione al termine della collaborazione professionale.

Inoltre, stabilisce le regole interne in relazione alla protezione dei dati personali e delle informazioni in generale, agli obblighi di riservatezza, e quindi alle regole di gestione delle attività quotidiane afferenti a quanto sopra indicato.

Il regolamento si applica sia ai lavoratori interni che ai collaboratori esterni, senza distinzione di ruolo, inquadramento, contratto, modalità di assunzione e/o livello, salvo quanto espressamente specificato nel presente regolamento e con riferimento all'intero novero di strumenti, servizi e apparati informatici e di gestione/trattamento di dati ed informazioni, anche se non ancora diffusi sul mercato, che rientrano o rientreranno nella definizione di "Rete Informatica" e/o "Risorse ICT" o che, più genericamente, potranno comportare rischi e problemi come riportato in premessa.

Oltre alle prescrizioni di cui al presente regolamento, tutti i soggetti appena richiamati sono tenuti al rispetto anche delle regole di "buon senso", ovvero la cura ed il rispetto propri del "buon padre di famiglia", in relazione a beni (*asset*) che non sono propri e che l'organizzazione considera strategici e vitali per il proseguo delle normali attività.

Qualunque violazione delle regole o dei concetti esposti sarà valutata, ed eventualmente sanzionata con provvedimenti disciplinari e risarcitori nel caso di personale lavoratore, nonché attraverso gli appositi rimedi contrattuali nel caso di collaboratori esterni e/o fornitori.

Nella gestione dei dati personali e delle informazioni, e in relazione alla sicurezza e al trattamento di questi, è necessario un impegno costante da parte di tutti, a tutti i livelli.

Premesso che ogni lavoratore e/o collaboratore deve trattare dati e informazioni quotidianamente per espletare le normali attività, si riporta quanto citato dalla norma internazionale ISO 27001.

"Tutto il personale è responsabile dei beni dati loro in concessione d'uso, sebbene non esclusivo, sia materiali che immateriali, compresi i software e le credenziali di accesso ovvero la posta elettronica. Il personale deve essere un elemento proattivo nella gestione della sicurezza, identificando, analizzando e riferendo su oggetti, fenomeni, procedure che rappresentino un rischio per il corretto trattamento delle informazioni. Qualsiasi persona ha l'obbligo formale e morale di comunicare alla direzione attraverso i canali più appropriati qualsiasi violazione delle policies interne sulla sicurezza informativa, indipendentemente da cosa, chi, perché o come sia avvenuta la violazione riscontrata."

Infine, il presente regolamento sostituisce e annulla il precedente, disposizione e/o prassi adottata, in qualsiasi forma comunicata con riferimento alle materie qui disciplinate, è applicabile anche alle figure politiche che utilizzano strumenti informatici della Organizzazione, fatta eccezione per la parte relativa alle sanzioni.

1.2 Aggiornamento e revisione

La presente policy è soggetta a revisione almeno annuale.

1.3 Figure e ruoli all'interno dell'organizzazione

Nel presente documento sono richiamate figure professionali (interne e/o esterne) che operano all'interno e/o per conto dell'organizzazione su argomenti di cui questo regolamento costituisce la sintesi.

Tali figure sono:

- dirigenti;
- responsabili di funzione e/o posizione organizzativa;
- responsabile ICT;
- amministratore di sistema (o amministratori);
- responsabile della protezione dei dati;

Incidono, inoltre, sull'operatività dell'organizzazione i seguenti soggetti esterni:

- responsabile del trattamento;
- titolare del trattamento.

2. DICHIARAZIONI GENERALI

2.1 Accesso da remoto ai sistemi informativi

Tutti i lavoratori e/o collaboratori esterni accettano che, per motivi di assistenza, manutenzione, ricerca di virus, attività di indagine sui malfunzionamenti, ricerca di anomalie o altre esigenze dell'organizzazione, la struttura ICT possa accedere da remoto sui dispositivi collegati alla rete interna o dall'esterno mediante connessioni sicure.

L'accesso sul dispositivo da parte della struttura ICT, di regola, viene concordato con il lavoratore e/o collaboratore che ne richiede la teleassistenza. Tuttavia, in talune circostanze dettate da comprovata urgenza, lo staff ICT potrà collegarsi sui sistemi senza nessuna specifica autorizzazione preventiva o comunicazione in tal senso.

L'accesso remoto dall'esterno mediante connessioni sicure è strettamente legato all'autorizzazione del personale ICT e alla fattibilità tecnica di creare un collegamento sicuro verso la rete interna.

2.2 Controlli di sistema

Tutti i sistemi informatici interni sono configurati per effettuare dei LOG sulle attività e sulla connettività, al fine primario di tutelare la sicurezza informatica dell'organizzazione. Tali sistemi di registrazione includono gli accessi ai sistemi, alla posta elettronica, alle connessioni di rete verso sistemi interni, alle connessioni di rete verso host esterni, all'utilizzo di file all'interno delle cartelle condivise, ecc.

Potenzialmente, la struttura ICT può sottoporre a osservazione e monitoraggio qualsiasi asset interno senza che questo sia comunicato preventivamente all'utilizzatore del bene.

I dati contenuti nel LOG sono assolutamente anonimi ma sono in grado di identificare il PC e/o l'utente collegato in locale a una connessione a servizi interna o esterna.

In tal senso, la registrazione dei LOG non viene effettuata per fare un controllo ordinario dell'attività del lavoratore, bensì per effettuare opportune indagini nel momento in cui ciò si renda necessario.

In caso quindi, non sia assolutamente necessario e/o specificatamente richiesto, i LOG non saranno sottoposti ad analisi né saranno visionati dalla direzione, dall'amministratore di sistema o da qualsiasi altra persona fisica e/o giuridica.

2.3 Dichiarazione di proprietà degli strumenti/risorse informative

Le risorse informative interne (fisiche, logiche o virtuali – asset, dato o informazioni) sono e rimarranno di proprietà dell'organizzazione e l'assegnazione e disponibilità delle stesse sono "temporanee", nonché limitate all'esclusivo uso professionale. L'assegnazione delle risorse non implica un trasferimento del diritto di proprietà, di usufrutto, di comodato d'uso delle stesse, né provoca la nascita di un diritto di esclusiva sull'utilizzo, né tantomeno deve essere considerata come benefit sulla retribuzione o come autorizzazione all'utilizzo promiscuo.

In caso di comprovata necessità, ad esempio in caso di assenza prolungata imprevista o di necessità al fine della continuità operativa, l'organizzazione può:

- revocare l'utilizzo;
- cancellare i dati;
- assegnarli ad altro personale;
- modificarne gli accessi;
- modificarne le condivisioni;
- svolgere attività di controllo, amministrazione, backup;
- condividere le informazioni e i dati con altri collaboratori.

2.4 Regole generali in materia di domicilio informatico-digitale, identità digitale e posta elettronica

La riservatezza di una casella di posta elettronica "personale privata" è tutelata a livello costituzionale, penale e dalla legge sulla privacy. Tuttavia, quando la casella di posta è messa a disposizione da parte dell'organizzazione, quest'ultima potrebbe avere la necessità di accedere alle informazioni ivi contenute, al fine di garantire la corretta prosecuzione delle attività professionali proprie.

Questo concetto si applica, non solo in modo specifico alle caselle di posta di tipo condiviso, quali per es. amministrazione@finpiemonte.it, risorse.umane@finpiemonte.it, ma anche alle caselle di posta nominali quali nome.cognome@finpiemonte.it. L'indirizzo nome.cognome@finpiemonte.it non appartiene a colui identificato quale "nome.cognome", bensì alla proprietaria del dominio, ovvero "finpiemonte.it".

2.5 Custodia delle risorse

Le Risorse ICT interne (per esempio PC portatili, smartphone, ecc.) affidate ai lavoratori o collaboratori esterni devono essere custodite con cura ed in modo appropriato, evitando ogni possibile forma di danneggiamento, manomissione o utilizzo da parte di soggetti terzi non autorizzati. Il furto, il danneggiamento o lo smarrimento delle Risorse ICT interne devono essere prontamente segnalati all'organizzazione, attraverso l'Allegato B "Data Breach interno".

Le Risorse ICT interne non devono essere lasciate incustodite durante una sessione di trattamento dei dati. L'accesso alla postazione di lavoro deve essere bloccato ogni qual volta ci si allontani da essa. Il sistema deve essere sempre sotto controllo.

Al termine della giornata lavorativa, in caso di assenze prolungate o in caso di suo inutilizzo, il PC e le relative periferiche (monitor, stampanti, ecc.) devono essere spenti.

2.6 Divieti generali

Non è consentito utilizzare strumenti software e/o hardware, facenti parte delle Risorse ICT, atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti in qualsiasi forma e memorizzati in qualsiasi modalità, all'interno o all'esterno della rete dell'organizzazione.

Non è consentita alcuna modificazione o alterazione dei sistemi operativi e delle configurazioni delle Risorse ICT, non è consentito disinstallare, modificare, reinstallare, alterare o cedere/distribuire a terzi il sistema operativo ovvero qualsiasi altro software fornito in dotazione dall'Organizzazione, specialmente quando tali modifiche possano compromettere la sicurezza della Rete ICT (ad es. disattivazione dell'anti-virus installato sul dispositivo) o violare la disciplina in tema di copyright.

L'Organizzazione si riserva la facoltà di modificare configurazioni, sistemi operativi e impostazioni delle Risorse ICT, anche procedendo alla formattazione delle stesse, in qualsiasi momento.

2.7 Utilizzo condiviso degli strumenti dell'organizzazione

Qualora una risorsa infrastrutturale sia utilizzata da più autorizzati, è necessario ricordare, ogni volta che si è terminato di utilizzare la stessa, di disconnettersi dal sistema effettuando il logout del proprio profilo personale.

Prima di effettuare la disconnessione, si dovranno chiudere i programmi rimasti eventualmente aperti. In questo modo, la persona che utilizza il PC, dovrà in seguito in ogni caso effettuare la procedura di autenticazione.

2.8 Interruzione del rapporto di lavoro

Al momento della cessazione del rapporto lavorativo e in tutti gli altri casi in cui ciò sia richiesto, il lavoratore ha l'obbligo di riconsegnare immediatamente la risorsa infrastrutturale allo stato in cui si trova.

2.9 Cessazione dei servizi

Ai sensi del presente regolamento, le credenziali di accesso alla rete informatica interna, a specifici software, così come l'utilizzo del servizio di accesso ad internet e di utilizzo della posta elettronica, potranno cessare, anche temporaneamente, nei seguenti casi:

a) se non sussiste più la condizione di lavoratore/collaboratore autorizzato o non è confermata l'autorizzazione all'uso;
b) se è accertato un uso non corretto delle risorse informatiche da parte dell'utente o comunque un uso estraneo ai suoi compiti professionali;
c) se vengono sospettate manomissioni e/o interventi sul hardware e/o sul software da parte dell'utente, eventualmente per il tramite di personale non autorizzato;
d) in caso di diffusione o comunicazione, imputabili direttamente o indirettamente all'utente, di password e/o altre informazioni tecniche riservate;
e) in caso di accesso doloso dell'utente a directory, a siti e/o file e/o servizi da chiunque resi disponibili non rientranti fra quelli per lui autorizzati e in ogni caso qualora l'attività dell'utente comporti danno, anche solo potenziale;
f) in ogni altro caso in cui sussistono ragionevoli evidenze di una violazione degli obblighi dell'utente.

2.10 Obbligo alla riservatezza e al segreto professionale

Per informazioni riservate (di seguito, le "Informazioni") si intendono tutte le informazioni di qualsivoglia natura riferite all'Organizzazione, ai soggetti esterni coinvolti (ad es. Fornitori) e a qualsiasi collaboratore coinvolto, anche indirettamente.

L'informazione è sempre classificata come "riservata" salvo quanto disposto successivamente.

L'informazione può essere di qualsiasi forma, ossia verbale, scritta, informatica, digitale, immagini, suoni, ecc.

Con riferimento alla riservatezza delle Informazioni, ogni soggetto esterno si impegna irrevocabilmente a non divulgare le informazioni riferite all'Organizzazione. Il soggetto esterno si impegna inoltre affinché anche i suoi dipendenti e consulenti esterni garantiscano la predetta riservatezza delle informazioni.

Nel caso in cui, per vincoli di legge o per regolamentazioni di Autorità competenti, sia necessario inviare delle informazioni a terzi è necessario comunicare tale esigenza all'interno dell'organizzazione al fine di concordare tempi e modalità di divulgazione.

Nella gestione ordinaria e straordinaria delle attività, tutti i lavoratori/collaboratori sono tenuti a garantire la massima riservatezza in relazione alle informazioni, dati o altro usati o trattati per la loro attività o di cui vengano a conoscenza, direttamente o indirettamente.

L'articolo 622 del codice penale prevede che tutte le informazioni spedite e ricevute da ogni singolo collaboratore dovrebbero essere protette dal segreto d'ufficio o professionale, stabilendo il principio della prudenza, ovvero che ogni attività non esplicitamente prevista e autorizzata risulta essere sanzionabile. E' pertanto tassativamente proibita la comunicazione o diffusione a persone o entità estranee all'organizzazione qualora la stessa non sia stata esplicitamente prevista e autorizzata (principio della prudenza).

La stampa dei messaggi o informazioni deve essere contenuta a quanto strettamente necessario per una corretta consultazione. Di norma, il documento cartaceo deve essere distrutto dopo la consultazione, salvo che esso sia utile per usi tecnici o di documentazione all'interno di specifici dossier.

La riservatezza si estende anche a informazioni riguardanti personale, collaboratori, clienti/utenti e fornitori dell'organizzazione.

2.11 Obbligo alla condivisione ed informazione

Tutto il personale, a qualsiasi livello, e tutti i collaboratori hanno l'obbligo di comunicare al proprio responsabile e/o alla struttura ICT, azioni, situazioni, pericoli, rischi, procedure (interne e/o esterne), stati di fatto, interazioni, attività o altro che possano comportare un rischio per la sicurezza dei dati e delle informazioni.

In questo, ed in altri frangenti, fenomeni di tipo omertoso non sono ammessi e tali atteggiamenti saranno, ove possibile, sanzionati.

In tutte le attività deve essere sempre presente una visione alla determinazione del "rischio" in modo tale che l'organizzazione possa in questo modo fare tesoro dell'esperienza e del punto di vista di ogni collaboratore.

3. REGOLE SPECIFICHE

3.1 Copie delle informazioni e gestione supporti strumenti portatili

3.1.1 Introduzione generale

La copia dei dati personali e di informazioni deve essere effettuata usando un approccio alla sicurezza attivo e secondo criteri di assoluta necessità.

L'organizzazione mette a disposizione una struttura di "repository" (ovvero di "magazzino") per le informazioni e per i dati, tale per cui ne siano garantite:

- riservatezza (garanzia che le informazioni siano accessibili solo da parte delle persone autorizzate);
- integrità (salvaguardia dell'accuratezza e della completezza);
- disponibilità (garanzia che gli utenti autorizzati abbiano accesso alle informazioni ed alle risorse associate solo quando ne hanno bisogno).

La copia di un'informazione al di fuori dei luoghi preposti espone l'organizzazione a un considerevole rischio che non siano garantite le caratteristiche sopra indicate (per esempio accesso alle informazioni contenute in Pen Drive, HD esterni, file salvati in locale sui PC, anche in caso di formattazione semplice da parte di un esperto del settore). Quindi la copia delle informazioni deve essere considerata un evento residuale e deve essere effettuata solo se non esistono alternative perseguibili.

3.1.2 Regole specifiche

In particolare, si riportano le seguenti regole di condotta da osservare.

1) Evitare di copiare, trasferire, o muovere file dai server o NAS interne all'interno di PC portatili o supporti removibili. Si deve usare il principio della assoluta necessità e della massima prudenza. Dunque i file possono essere copiati solo per esigenze eccezionali, per poi riportali sui server dell'organizzazione, eliminandoli dal dispositivo portatile.
2) È fatto divieto di utilizzare supporti rimovibili personali (Pen Drive USB, dischi esterni, ecc.). Vengono disattivate l'apertura automatica dei messaggi di posta elettronica e l'anteprima automatica dei contenuti dei file sempre dalla posta elettronica.
3) La memorizzazione dei dati dell'organizzazione sulle Pen Drive deve essere esclusivamente a carattere temporaneo (nell'ordine delle poche ore) e la stessa deve essere oggetto di formattazione immediata dopo l'utilizzo temporaneo del file memorizzato. Le Pen Drive devono essere tassativamente rilasciate senza alcun file al loro interno.
4) Solo le Pen Drive fornite dall'Organizzazione possono essere utilizzate per una copia o per trasferire temporaneamente i dati da un dispositivo all'altro.
5) Non lasciare mai incustodito un dispositivo portatile, in particolare non lasciare mai sulla scrivania, facilmente accessibili, pen drive o HD esterni; questi vanno sempre chiusi a chiave in cassetti o armadi o comunque gestiti alla stregua di uno smartphone o PC Portatile.
6) Deve essere sempre applicata la policy del "*bring the device always with you*", ovvero non lasciare incustodito un dispositivo, in macchina, presso clienti in area non controllata, in sala riunioni non chiusa a chiave, ecc.
7) Tenere sempre in considerazione il fatto che un asset fisico (per esempio un PC portatile o Smartphone) può essere sempre rimpiazzato o acquistato nuovamente; al contrario, il suo contenuto (in termini di dati ed informazioni) non è "acquistabile" né "rimpiazzabile".
8) Non trascrivere informazioni sensibili (login, password, ecc.), né in forma cartacea né in forma elettronica, all'interno di un dispositivo, a meno che questo non avvenga mediante opportuna procedura di crittazione dei dati.
9) Per i medesimi motivi, lo scambio di informazioni e/o di dati anche all'interno dell'organizzazione dovrebbe avvenire mediante condivisione della risorsa all'interno dei server e/o delle NAS interne, piuttosto che per posta elettronica e/o mediante l'uso di dispositivi removibili.
10) Non usare dispositivi come Pen Drive o hard disk esterni per il salvataggio *primario* di file di lavoro invece di usare i supporti interni al PC o alla rete aziendale.

3.1.3 Misure specifiche a tutela riservatezza, integrità, disponibilità e resilienza della rete telematica– backup

Al fine di garantire riservatezza, integrità, disponibilità e resilienza della rete ICT interna, delle singole postazioni dell'ente e della server farm sono stati installati ed attivati strumenti generali di difesa informatica per:

- adottare un controllo degli accessi logici (in ingresso ed in uscita);
- garantire l'accesso autorizzato alle risorse informatiche;
- utilizzare sistemi ridondanti a diversi livelli per garantire continuità nell'erogazione dei servizi;
- integrare politiche di backup;
- adottare misure tecniche ed organizzative per minimizzare le interruzioni di servizio.

3.2 Politica del Clean Desk e Clean Desktop

3.2.1 Introduzione generale

Una politica di Clean Desk e Clean Desktop è uno strumento molto importante per garantire che tutti i materiali sensibili e le informazioni anche confidenziali siano rimosse da un utente dopo il loro utilizzo.

3.2.2 Regole specifiche

Di seguito vengono elencati divieti/regole specifici di applicazione della politica di Clean Desk e Clean Desktop.

A. DIVIETI

1) Lasciare documenti cartacei visibili sulla scrivania e sul posto di lavoro anche dopo che il titolare o "custode" dei documenti si sia reso assente.
2) Stampare e lasciare stampe e documenti cartacei in giro senza preoccuparsi di proteggere le informazioni ivi contenute, anche all'interno della stampante.
3) Lasciare in giro o sul proprio posto di lavoro supporti di memorizzazione che contengono dati o informazioni dell'organizzazione (CD ROM DVD, Pen Drive, HD esterni, memorie SD ecc.).
4) Dimenticarsi di documenti o di supporti di memorizzazione in giro per l'ufficio e, con aspetti molto più importanti dal punto di vista della sicurezza, scordarseli da un Cliente, Fornitore o terzo che sia.
5) Lasciare incustoditi (logicamente o fisicamente) file o documenti cartacei che riportino informazioni altamente riservate come password o criteri di accesso ai sistemi.
6) Lasciare la propria postazione attiva senza un blocco logico in modo che nessuna possa operare sulla sessione di lavoro aperta da un altro.
7) Tenere copie di documenti sul proprio desktop "logico" del PC che non siano strettamente necessari alla fase di modifica.
8) Fare eccessive copie di file e documenti, perdendo completamente la gestione delle revisioni e rendendo impossibile sapere se un documento è quello in corso o meno.

B. REGOLE

1) Limitare l'utilizzo di scanner o copia per documenti critici e/o ad alto rischio od impatto sulla sicurezza complessiva.
2) Le informazioni critiche, per esempio su carta o su supporti di memorizzazione digitale, quando non utilizzate, dovrebbero essere chiuse a chiave (idealmente in cassaforte o armadio o altri mobili con caratteristiche di sicurezza) soprattutto quando l'ufficio è vuoto. Nello specifico, è opportuno fare riferimento alle seguenti accortezze.
    i. Non si devono lasciare collegati computer e terminali o questi devono essere protetti, quando incustoditi, con un salva-schermo e meccanismi di blocco della tastiera controllati con una password o token o con altri meccanismi similari di autenticazione dell'utente.
    ii. Le stampe contenenti informazioni riservate o classificate devono essere rimosse immediatamente dalle stampanti.
    iii. Tutti sono tenuti a garantire che tutti i dati (particolari o meno) e tutte le informazioni in formato cartaceo o elettronico devono essere posti nella area di lavoro alla fine della giornata e quando ci si assenta per un periodo di tempo prolungato.
    iv. Tutti i computer devono essere bloccati quando l'area di lavoro non è occupata.

v. Tutti i computer devono essere spenti quando si è al termine della giornata lavorativa. In talune circostanze deve essere valutato lo spegnimento anche durante la giornata se la postazione di lavoro non verrà usata per due ore o più.

vi. Tutte le informazioni devono essere rimosse dalla scrivania e, al limite, chiuse in un cassetto quando la scrivania non è presidiata e alla fine della giornata di lavoro.

vii. Gli armadi contenenti informazioni *sensibili* devono essere mantenuti chiusi e bloccati quando non sono in uso e non sono presidiati a vista.

viii. Strumenti di accesso quali chiavi digitali, token, smart card, ecc. (utilizzati per accedere a informazioni riservate o ristrette) non devono essere mai lasciate incustodite. In taluni casi, è opportuno portare sempre con sé tali dispositivi, ma mai in una borsa o borsello da dove possono essere sottratti.

ix. Se previsto ed in talune circostanze, i computer portatili devono essere bloccati con un cavo anti effrazione o chiusi a chiave in cassetti o armadi.

x. La password non può essere lasciata su foglietti adesivi postati su un computer, né possono essere scritti e mantenuti in una posizione facilmente accessibile. La login e la password sono una informazione strettamente riservata che dovrà essere imparata a memoria senza trascriverla in nessun modo ed in nessuna locazione.

xi. Stampe contenenti informazioni *sensibili* devono essere immediatamente rimosse dalla stampante.

xii. I documenti riservati e/o ad accesso limitato devono essere distrutti nel distruggi documenti e non lasciati senza protezione.

xiii. Lavagne contenenti informazioni devono essere cancellate ed i fogli distrutti.

xiv. Bloccare immediatamente i dispositivi informatici portatili come i laptop e tablet subito dopo il loro uso, anche per assenze temporanee molto brevi.

xv. Trattare i dispositivi di archiviazione di massa come CD-ROM, DVD, o unità USB / Pen Drive come critici e chiuderli sempre in un cassetto o armadio.

xvi. Identificare sempre le Pen Drive utilizzate, in modo che un loro furto possa essere sempre identificato. Spesso la sottrazione di dati avviene senza che il proprietario se ne renda conto.

xvii. Usare i dispositivi di memorizzazione di massa esterni come repository temporanea, formattandoli sempre dopo un utilizzo.

xviii. Non copiare sul PC, Notebook, memorie esterne documenti e/o informazioni dell'organizzazione; le attività devono essere espletate utilizzando i dati all'interno della rete e nei posti consentiti. La copia delle informazioni sui dispositivi periferici è e deve essere una eccezione, limitata all'uso per ore o pochi giorni.

3.3 Limitazioni all'installazione e all'utilizzo di software

3.3.1 Introduzione generale

All'interno dell'organizzazione, in merito all'installazione/utilizzo dei software, la struttura ICT ha la responsabilità di:

- valutare le necessità in ambito ICT;
- scegliere la soluzione più idonea;

- valutare l'impatto sulla sicurezza;
- acquistare il software necessario;
- gestire le licenze;
- provvedere all'installazione dei PC e relativa manutenzione;
- gestire gli aggiornamenti;
- valutare l'acquisto di nuove versioni per adeguamento a criteri di sicurezza o funzionalità.

3.3.2 Regole specifiche

Alla luce della predetta responsabilità esclusiva della struttura ICT, è vietato l'utilizzo/installazione di qualsiasi software/applicazione non precedentemente autorizzato dallo staff ICT.

In particolare i software installati sulle postazioni devono essere quelli autorizzati dall'amministrazione e provvisti di regolare licenza.

Con apposita richiesta, il responsabile di Area dovrà richiedere l'autorizzazione di installazione per software necessari ai fini lavorativi.

3.4 Policy autenticazione – Login - Password

3.4.1 Introduzione generale

L'accesso alla rete informatica interna è limitato ai lavoratori e agli altri soggetti espressamente autorizzati dall'organizzazione nella figura della struttura ICT.

3.4.2 Regole specifiche

3.4.2.1 Regole di accesso

L'autorizzazione all'accesso al sistema informativo è dato dalla struttura ICT interna. Nessuno al di fuori della stessa è autorizzato a rilasciare accessi o password atti ad accedere a qualunque sistema, compreso il Wi-Fi.

Username e password per accedere alla rete ICT interna o a risorse digitali in qualsiasi forma, sono strettamente personali e il lavoratore o collaboratore sono tenuti a tutelare e a mantenere la segretezza delle proprie credenziali di accesso.

La prima password di accesso viene fornita all'utente direttamente dal sistema ICT. Tale password dovrà essere cambiata al primo accesso da parte dell'utente stesso, secondo le regole di cui al successivo punto, e viene custodita secondo le modalità più opportune definite dallo staff ICT. Lo staff ICT al momento adotta una procedura per la custodia delle credenziali di rete e disponibile in rete.

3.4.2.2 Regole di password change

Il lavoratore è tenuto a sostituire la propria password ogni qualvolta sospetti che la stessa non sia più segreta. La password ha una durata di 90 giorni trascorsi i quali è necessario il cambio.

Nel caso in cui, per motivi tecnici od organizzativi, non sia possibile cambiare in autonomia la password ai sistemi, è responsabilità di ogni collaboratore richiedere l'intervento della struttura ICT.

Le password devono essere formate da lettere (maiuscole o minuscole, con rilevanza ai fini del sistema), numeri e i caratteri speciali; devono essere composte da almeno otto caratteri alfanumerici di cui almeno un numero, una lettera maiuscola, una lettera minuscola e un carattere speciale e non devono contenere riferimenti agevolmente riconducibili al soggetto interessato.

Le password non devono contenere nomi o parti di nomi comuni (es. PIPPO, GIOVA, MARIA ecc.), sequenza di caratteri troppo semplici (es. ABCD, QWERTY, 12345 ecc.) o riferimenti alla propria sfera personale (es. Data di Nascita, parti del codice fiscale, nomi dei figli ecc.).

Per una maggiore flessibilità nelle attività operative e nella gestione del sistema ICT, è data facoltà al personale di modificare secondo schemi e regole prestabilite la password di accesso ai sistemi informativi.

Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia alla Direzione (o persona da questa incaricata) o alla struttura ICT, oppure al custode delle password, ove previsto.

3.4.2.3 Regole di disattivazione

Le credenziali di autenticazione alla rete aziendale non utilizzate da almeno tre mesi sono disattivate (per la disattivazione delle credenziali occorre l'autorizzazione da parte dell'ufficio Risorse Umane), salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica, organizzativa o di servizio; anche in questo caso la struttura ICT si fa garante della gestione degli account tecnici utilizzati.

3.5 Utilizzo rete ICT interna

3.5.1 Introduzione generale

La rete ICT interna è rappresentata dagli strumenti, apparecchiature, software o quant'altro sia utilizzabile per "comunicare" e per gestire "informazioni". Da questo l'acronimo ICT, ovvero Information & Communication Technology.

Tutte le considerazioni e regole relative alla rete ICT interna sono applicabili anche alla rete WIFI.

3.5.2 Regole specifiche

È vietata la navigazione sulla rete internet per scopi diversi da quelli strettamente legati all'attività professionale, sia attraverso le Risorse ICT, sia attraverso connessioni Internet personali.

La regola sopra descritta deve ritenersi valida anche per l'utilizzo di "app" installate su smartphone, tablet e smartwatch, che, per il loro funzionamento, accedano alla rete ICT interna.

L'organizzazione, al fine di evitare la navigazione su siti web non pertinenti all'attività lavorativa, si riserva la facoltà di inserire un blocco e/o un filtro automatico in grado di impedire l'accesso a determinati siti web che saranno indicati in una "blacklist", ovvero ai contenuti o alla classificazione dei siti web consultati.

Le precedenti disposizioni e i predetti divieti trovano applicazione, per quanto possibile anche all'utilizzo di dispositivi personali di collaboratori esterni durante l'orario di lavoro e ferma ogni altra disposizione di legge in materia.

3.6 Uso di dispositivi personali

Il lavoratore può collegare un suo dispositivo, anche mobili (come lo smartphone) alla rete interna solo a seguito di una esplicita autorizzazione della funzione ICT.

Nel caso in cui gli utenti abbiano configurato posta elettronica e altre app fornite dall'ente sui propri supporti mobile (smartphone, tablet ecc.), dovranno obbligatoriamente proteggere l'accesso al dispositivo con credenziali o PIN.

3.7 Posta elettronica e messaggistica

3.7.1 Introduzione generale

L'invio di un messaggio, poiché effettuato attraverso un PC dedicato per ogni singolo utente, identifica l'autore in modo automatico attraverso la password preventivamente inserita al momento del richiamo dell'applicazione. Ne consegue che, come per una comune lettera, l'autore del messaggio deve essere fisicamente la persona che riveste i poteri per effettuare la comunicazione medesima, ovvero colui che ha effettuato l'accesso al sistema mediante la sua login e password.

Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. Pertanto è fatto divieto di utilizzare le caselle di posta elettronica facenti riferimento al dominio dell'organizzazione o in qualche modo alla stessa riconducibile, per l'invio di messaggi a interlocutori personali e/o con contenuti non strettamente necessari per l'attività professionale.

In caso di necessità per l'utilizzo di risorse quali Skype, Whatsapp ed altri strumenti di messaggistica, è necessario contattare i tecnici ICT per le valutazioni tecniche del caso.

Ai collaboratori esterni non viene assegnata una casella di posta dell'organizzazione, a meno di specifiche eccezioni espresse allo staff ICT dalla direzione.

3.7.2 Regole specifiche

In caso di assenze programmate, il lavoratore provvederà ad impostare la funzione di risposta automatica per la propria casella di posta interna, fornendo nel messaggio tutte le indicazioni utili alla corretta prosecuzione dell'attività lavorativa in sua assenza e, in particolare, il recapito mail del proprio sostituto *pro tempore* e, se pertinente, del proprio diretto superiore gerarchico.

In caso di assenze non programmate, qualora l'impostazione della funzione di risposta automatica non venisse attivata entro 24 ore dal collaboratore stesso, l'Organizzazione si riserva la facoltà di provvedere a tale incombenza mediante l'intervento della sua struttura ICT, anche modificando temporaneamente la password di accesso.

Nel caso in cui il lavoratore e/o collaboratore non lavorino od operino più all'interno dell'organizzazione (per qualsiasi motivo, ivi compresa la cessazione del rapporto di lavoro), quest'ultima manterrà la casella di posta del collaboratore attiva per tre mesi, previa modifica della password di accesso. In tali casi verrà impostato, da parte dell'organizzazione, un messaggio automatico in cui siano fornite tutte le indicazioni utili alla corretta prosecuzione dell'attività lavorativa e, in particolare, il recapito mail del collaboratore di riferimento in sostituzione.

Decorsi tre mesi, l'account verrà disabilitato, disattivando anche il messaggio di risposta automatica.

Nessuna comunicazione sarà garantita al collaboratore la cui casella di posta sia stata revocata e/o reindirizzata verso un altro destinatario.

Tutte le disposizioni relative alla casella di posta elettronica interna assegnata al lavoratore devono ritenersi valide, per quanto compatibili, anche per qualsiasi altra forma di messaggistica/corrispondenza scritta inviata e/o ricevuta attraverso la rete ICT e/o mediante una risorsa ICT. A titolo di esempio si considerano strumenti di messaggistica istantanea le caselle di posta elettronica certificata (PEC), gli SMS, Skype dell'organizzazione, etc.

4. SISTEMA DI CONTROLLI GRADUALI

In caso di violazione delle disposizioni del presente Regolamento l'Organizzazione può procedere a verificare, nei limiti consentiti dalle norme legali e contrattuali e nel rispetto dei diritti dei lavoratori, l'integrità della propria Rete Informatica e l'ottemperanza alle disposizioni di Legge e contrattuali, in quanto sia l'Organizzazione sia il singolo dipendente sono penalmente sanzionabili.

Le verifiche possono essere effettuate a norma dell'articolo 4 dello Statuto dei Lavoratori che prevede che sia gli impianti audiovisivi, sia altri strumenti di controllo a distanza possono essere installati «*esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio interno*», in base a uno specifico accordo sindacale.

Mentre per quanto riguarda gli strumenti informatici/tecnologici in dotazione al lavoratore per svolgere l'attività lavorativa (PC, Notebook, tablet, smartphone, badge elettronici, etc.) l'Organizzazione può effettuare verifiche a distanza senza dover definire un accordo sindacale o una preventiva autorizzazione amministrativa, come previsto dal comma 2 art. 4 dello Statuto dei lavoratori.

L'Organizzazione può controllare tutte le Risorse ICT interne e i lavoratori, accedendo a dati e a conversazioni sui dispositivi interni usati dagli stessi, le informazioni così raccolte saranno utilizzabili a tutti i fini connessi al rapporto di lavoro, inclusa la facoltà di emettere provvedimenti disciplinari.

In altre parole, tutte le Risorse ICT interne possono essere controllate a distanza. L'organizzazione intende procedere a tali controlli a distanza delle Risorse ICT dei lavoratori. La stessa potrà, pertanto, accedere a dati e a conversazioni sui dispositivi interni. Le informazioni così raccolte saranno utilizzabili a tutti i fini connessi al rapporto di lavoro, inclusa la facoltà di emettere provvedimenti disciplinari.

Qualora le misure tecniche preventive adottate dall'Organizzazione non fossero sufficienti ad evitare eventi dannosi o situazioni di pericolo, la stessa effettuerà con gradualità, nel rispetto dei principi di pertinenza e non eccedenza, le verifiche di eventuali situazioni anomale attraverso le seguenti fasi:

a) analisi aggregata del traffico di rete riferito all'intera Rete Informatica o a sue aree (reparto, servizio, ecc.), rilevazione della tipologia di utilizzo (e-mail, file audio, accesso a risorse estranee alle mansioni), dei dati memorizzati sui server a livello di intera struttura lavorativa (reparto, servizio, ecc.) e rilevazione della tipologia di utilizzo (file audio, file video, immagini, software non autorizzato) e relativa pertinenza con l'attività lavorativa;

b) emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo degli strumenti interni, con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite; il richiamo all'osservanza delle regole può essere circoscritto agli operatori afferenti al settore in cui è stata rilevata l'anomalia;

c) in caso di successivo permanere di una situazione non conforme e, in caso di abusi singoli e reiterati si eseguiranno controlli nominativi o su singoli dispositivi e/o postazioni di lavoro. Sarà possibile procedere con un'analisi puntuale ed una eventuale eliminazione del materiale non conforme anche sulle singole postazioni di lavoro.

Fermo quanto sopra, l'accesso ai dati trattati dai lavoratori attraverso la Rete Informatica da parte dell'Organizzazione può avvenire, al di fuori di ogni finalità di controllo preventivo e sistematico dell'attività lavorativa e nel rispetto della normativa a tutela della privacy, anche per:

a) motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.);

b) controllo o programmazione dei costi;

c) comprovate esigenze manageriali o lavorative (ad es. accesso al computer del lavoratore per reperire file necessari all'attività lavorativa che siano conservati esclusivamente "in locale" su detto dispositivo, nel caso di assenza non programmata del lavoratore stesso);

d) verificare il corretto utilizzo da parte dei lavoratori tanto della rete internet che della posta elettronica, con la precisazione che in nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati;

e) permettere il libero accesso alle informazioni tanto della rete internet che della posta elettronica anche all'Autorità Giudiziaria richiedente.