REGOLAMENTO DI SICUREZZA INFORMATICA PER PERSONALE INTERNO

Teramo, 30 Giugno 2023

CRONOLOGIA REVISIONI E SINTESI MODIFICHE

Cronologia revisioni:

Rev.	Data	Descrizione
0	30.06.2023	Il Regolamento riporta le prescrizioni relative all'utilizzo delle risorse informatiche e telematiche a cui si devono attenere tutti i dipendenti e figure assimilate

Sintesi delle modifiche rispetto alla precedente versione:

Rev.	Descrizione

INDICE

NORMATIVA DI RIFERIMENTO E DISPOSIZIONI INTERNE 5

AMBITO DI APPLICAZIONE E PRINCIPI 6

Art. 1 - Introduzione 6

Art. 2 - Ambito di applicazione 6

Art. 3 - Principi generali 6

ACCESSO AL SISTEMA INFORMATICO 8

Art. 4 - Credenziali di autenticazione 8

Art. 5 - Gestione dei File 9

DISPOSITIVI INFORMATICI 10

Art. 6 - Dispositivi elettronici aziendali 10

Art. 7 - PC e computer portatili 11

Art. 8 – Licenze Software 11

Art. 9 - Supporti rimovibili 12

Art. 10 - Protezione da virus e da malware 12

Art. 11 - Strumenti di fonia mobile e/o di connettività in mobilità 13

Art. 12 - Stampanti, fotocopiatrici e fax 13

Art. 13 - Dispositivi elettronici personali 13

POSTA ELETTRONICA 14

Art. 14 - Finalità dell'utilizzo della posta elettronica 14

Art. 15 – Divieti e raccomandazioni 14

Art. 16 - Continuità del servizio e procedura di emergenza per l'accesso alla posta elettronica del lavoratore assente 15

Art. 17 - Controlli preventivi e successivi 15

RETE INTERNET 16

Art. 18 - Regole di utilizzo 16

Art. 19 - Divieti 16

Art. 20 - Controlli preventivi 16

Art. 21 - Controlli successivi 16

SOCIAL MEDIA 17

Art. 22 - Regole di utilizzo 17

Art. 23 - Divieti 17

GESTIONE DEGLI INCIDENTI DI SICUREZZA IT 18

Art. 24 - Prescrizioni 18

SISTEMA DEI CONTROLLI 19

Art. 25 - Finalità e modalita' di esecuzione 19

DISPOSIZIONI FINALI 20

Art. 26 - Sanzioni 20

Art. 27 - Aggiornamento e Revisione 20

Art. 28 - Entrata in vigore e diffusione 20

GLOSSARIO 21

NORMATIVA DI RIFERIMENTO E DISPOSIZIONI INTERNE

- Legge 20 maggio 1970, n. 300 “Statuto dei lavoratori”;
- D. Lgs. 30 giugno 2003, n. 196 “Codice in materia di protezione dei dati personali”;
- Regolamento (EU) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati - GDPR)”;
- D. Lgs. 10 agosto 2018, n. 101 recante “Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE”;
- D. Lgs. 7 marzo 2005, n. 82 “Codice dell’Amministrazione Digitale”;
- CCNL di settore;
- Linee guida e provvedimenti specifici del Garante per la Protezione dei Dati Personali;
- Circolare interna del 2005 (prot. 2941).

Titolo I

AMBITO DI APPLICAZIONE E PRINCIPI

ART. 1 - INTRODUZIONE

Il presente **Regolamento di Sicurezza informatica per il personale interno** (di seguito "**Regolamento**") riporta le prescrizioni relative all'utilizzo delle risorse informatiche e telematiche a cui si devono attenere tutti i dipendenti e figure assimilate[1] (di seguito i "**Dipendenti**" e, singolarmente, il "**Dipendente**") dell'*Istituto Zooprofilattico Sperimentale dell'Abruzzo e del Molise "G. Caporale"* (di seguito "**Istituto"**).

Questo al fine di tutelare i beni aziendali ed evitare comportamenti che potrebbero esporre l'*Istituto* a minacce di sicurezza e protezione dei dati trattati, di immagine e ripercussioni di tipo economico e patrimoniali per eventuali danni cagionati anche a terzi.

ART. 2 - AMBITO DI APPLICAZIONE

Il presente **Regolamento** si applica a tutti i Dipendenti, senza distinzione di ruolo o di livello.

Il presente **Regolamento**, nel rispetto delle vigenti disposizioni normative in tema di protezione dei dati personali e strumenti di controllo, ha altresì lo scopo di informare i Dipendenti – ai sensi dell'art. 12 e ss del Regolamento Europeo 2016/679 - sulle eventuali finalità e modalità dei controlli riferiti all'utilizzo degli strumenti informatici e sulle specifiche tecnologie adottate per effettuarli.

L'*Istituto* adotta il presente **Regolamento** anche al fine di adempiere agli obblighi fissati dall'art. 4 della Legge 20 maggio 1970 (*Statuto dei Lavoratori*), dal D.lgs. 196/2003 (*Codice in materia di protezione dei dati personali*) e dalle "*Linee guida del Garante per posta elettronica e internet – 10 marzo 2007*" emanato dal Garante per la protezione dei dati personali, e loro successive modificazioni e integrazioni.

ART. 3 - PRINCIPI GENERALI

L'utilizzo delle risorse informatiche e telematiche, nell'ambito dei rapporti di lavoro, deve sempre ispirarsi ai principi di diligenza e correttezza, con l'ulteriore finalità di prevenire eventuali comportamenti illeciti, pur nel rispetto dei diritti ad essi attribuiti dall'ordinamento giuridico italiano.

L'utilizzo delle risorse informatiche è consentito ai dipendenti solo per finalità di adempimento delle mansioni lavorative e, comunque, per l'esclusivo perseguimento degli obiettivi aziendali.
Sono vietati comportamenti che possano creare un danno, anche di immagine all'*Istituto*.
A tal fine ogni dipendente, nel rispetto dei principi di diligenza sottesi al rapporto instaurato con l'*Istituto*, è tenuto a tutelare (per quanto di propria competenza) il patrimonio aziendale

[1] - In questa categoria rientrano persone che pur non essendo inquadrate con un contratto di lavoro dipendente, ricoprono un ruolo in Azienda, come ad es.: lavoratori somministrati, stagisti, co.co.co., …

da utilizzi impropri e non autorizzati, danni o abusi anche derivanti da negligenza, imprudenza o imperizia. L'obiettivo è quello di preservare l'integrità e la riservatezza dei beni, delle informazioni e delle risorse aziendali.

Ogni dipendente è tenuto, in relazione al proprio ruolo e alle mansioni in concreto svolte, ad operare a tutela della sicurezza informatica aziendale, riportando al proprio **Responsabile** e senza ritardo eventuali rischi di cui è a conoscenza.

Il mancato rispetto delle prescrizioni di sicurezza contenute in questo **Regolamento** costituisce violazione dell'obbligo contrattuale.
Il dipendente dovrà, altresì, rispettare ogni ulteriore pertinente normativa fra cui, in particolare, la legislazione avente ad oggetto la tutela della riservatezza e del diritto d'autore, la disciplina inerente la responsabilità amministrativa della persona giuridica in caso di reati commessi da dipendenti, gli obblighi di fedeltà del dipendente e le disposizioni riguardanti i reati informatici.

Il dipendente deve utilizzare gli strumenti elettronici e telematici rispettando le seguenti regole di comportamento:

a. non deve introdursi in sistemi informatici o telematici ai quali non sia autorizzato ad accedere, in particolare se l'indebita intromissione o permanenza riguarda sistemi informatici o telematici protetti da misure di sicurezza;
b. non deve utilizzare o mettere a disposizione abusivamente codici di accesso o password o altri mezzi, i quali consentono di accedere, in modo logico o fisico, a sistemi informatici o telematici protetti da misure di sicurezza;
c. non deve utilizzare gli strumenti di comunicazione (quali, ad esempio, telefono fisso o mobile, posta elettronica, Internet o reti telematiche in genere tramite la fruizione di servizi interni e esterni di messaggistica o di condivisione dati) per offendere l'onore, il decoro o la reputazione di altri lavoratori o di terzi.

L'*Istituto*, in linea con quanto prescritto dall'ordinamento giuridico italiano (art. 4, Statuto dei Lavoratori), esclude la configurabilità di forme di controllo aziendali aventi direttamente ad oggetto l'attività lavorativa dell'utente. Tuttavia non si esclude che, per esigenze dettate dalla sicurezza del lavoro, dall'utilizzo dei sistemi informatici, impianti, apparecchiature o dispositivi possa derivare la possibilità di controllo a distanza dell'attività dei lavoratori. In tal caso, tali strumenti verranno valutati e subordinati rispetto alla normativa di settore ivi incluse le forme di partecipazione sindacale.

Titolo II

ACCESSO AL SISTEMA INFORMATICO

ART. 4 - CREDENZIALI DI AUTENTICAZIONE

Per permettere l'accesso alla rete dell'*Istituto* vengono assegnate al Dipendente specifiche credenziali di autenticazione (*username* e *password*) costituite da un codice identificativo dell'utente (*username*) associato ad una parola chiave (*password*) che consente di verificarne l'identità.

La password iniziale, assegnata in occasione del primo accesso, deve essere immediatamente modificata ad esclusiva cura del Dipendente. Successivamente la password deve essere obbligatoriamente modificata con la periodicità e le modalità previste.

Il sistema è configurato per controllare automaticamente la robustezza della *password* e per richiederne il cambio alla sua scadenza.

L'accesso ad una Applicazione può essere protetto da ulteriori credenziali che possono essere identiche o diverse da quelle di accesso alla Rete Aziendale.
Qualora diverse, devono sottostare ai vincoli previsti dall'Applicazione stessa.

In tutti i casi, la composizione della *password* deve seguire le regole previste, richieste e controllate dallo specifico software acceduto ed in particolare non deve essere comune e/o prevedibile, non deve coincidere con una sequenza banale di caratteri (ad es. 12345678) e non deve contenere riferimenti facilmente riconducibili al dipendente (ad es. nome, cognome, ecc.).

Le credenziali (*username* e *password*) sono strettamente personali, ovvero associate univocamente alla persona assegnataria. Devono essere custodite dal dipendente con la massima diligenza e non devono essere rivelate ad alcuno per nessun motivo.

In particolare la *password*:

- non deve essere memorizzata su file, appunti, post-it, …;
- deve essere digitata ogni volta.

Nel caso di sospetto che altri possano essere venuti a conoscenza della propria *password*, il Dipendente dovrà procedere immediatamente alla modifica della stessa e, contestualmente, segnalare l'evento (vedi *Capo V - Gestione degli Incidenti di Sicurezza IT*) per gli interventi del caso.

In caso di interruzione del rapporto di lavoro, le credenziali di autenticazione verranno disabilitate entro 24 ore da tale data.

Qualora, in funzione della criticità dei dati trattati e/o delle abilitazioni attribuite, vengano utilizzati sistemi di autenticazione a due fattori, il dipendente deve adeguarsi alle disposizioni che gli verranno di volta in volta impartite.

In assenza del Dipendente, in casi del tutto eccezionali in cui si rendesse indispensabile ed indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, l'*Istituto* si riserva la possibilità di utilizzare l'utenza personale del dipendente, previa

forzatura delle credenziali di accesso. Tale forzatura avviene esclusivamente nei casi e con le modalità previste dalla "*Procedura per la Forzatura di Utenze e Caselle Email*" che, in particolare, prevede l'avviso al dipendente oltre alla tracciatura delle autorizzazioni date e delle attività svolte.

ART. 5 - GESTIONE DEI FILE

Il Dipendente può essere autorizzato, in base al ruolo/mansione attribuito, ad accedere e/o gestire *file* memorizzati su determinate *cartelle di rete* posizionate sui *server* aziendali o sulle risorse Cloud dell'*Istituto*.

Le *cartelle di rete* e le risorse Cloud sono aree di condivisione di informazioni strettamente professionali e non possono essere in alcun modo utilizzate per scopi diversi. Pertanto qualunque *file* che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, su di esse.

Le *cartelle di rete* vengono accedute in base alle abilitazioni attribuite al Dipendente.

Sui *server* che ospitano le *cartelle di rete* vengono svolte dall'Amministratore di Sistema regolari attività di controllo e di amministrazione ed in particolare sono previsti periodici salvataggi dei dati (*backup).* Il salvataggio dei dati su copie di *backup* garantisce la possibilità di recuperare contenuti danneggiati e/o involontariamente rimossi.

Le risorse Cloud devono essere accedute esclusivamente con le modalità specificamente predisposte in funzione della tipologia di risorsa.

Per i dati memorizzati su tali risorse sono previsti periodici salvataggi dei dati (*backup).*

L'archiviazione di *file lavorativi* su cartelle locali (cioè su cartelle presenti sul proprio dispositivo) è consentita solo per brevi periodi, pari al tempo strettamente necessario per eseguire operazioni per cui sia necessaria tale archiviazione, e non è previsto alcun *backup*.

Non è consentita l'archiviazione di *file personali* in locale in quanto non può essere assicurata la riservatezza a fronte di situazioni eccezionali (es. interventi di assistenza, riparazioni, …).

Il personale tecnico con qualifica di *Amministratore di Sistema* può, in qualunque momento, procedere alla rimozione d'ufficio di elementi (*file* o *cartelle*) presenti in rete o su dispositivi individuali e ritenuti pericolosi per la sicurezza dell'ambiente di lavoro.

Titolo III
Capo I

DISPOSITIVI INFORMATICI

ART. 6 - DISPOSITIVI ELETTRONICI AZIENDALI

Ai fini del presente Regolamento si considerano equivalenti e sono riassunti sotto il termine di **dispositivi** i seguenti apparati:

- *Personal Computer* (PC) fisso o portatile;
- *Smartphone e Tablet*.

I dispositivi elettronici aziendali, di uso individuale, messi a disposizione dall'*Istituto*, sono strumenti di lavoro il cui utilizzo è determinato dalla necessità di svolgere attività inerenti alla prestazione di lavoro.

Consapevole di come tali dispositivi siano ormai divenuti parte integrante della vita quotidiana, l'*Istituto* non vieta in assoluto l'utilizzo personale di tali dispositivi purché ciò non pregiudichi la prestazione lavorativa e non contribuisca a innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

Ciascun dispositivo deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

Relativamente ai dispositivi portatili, il dipendente è tenuto a custodirlo con la massima diligenza sia durante l'utilizzo nel luogo di lavoro, sia al di fuori del luogo di lavoro o durante trasferte o spostamenti, adottando tutte le cautele necessarie per evitare danni o sottrazioni di dati, documenti o informazioni presenti nel PC stesso.
Al riguardo i veicoli (privati, aziendali, a noleggio, etc.) devono essere considerati come "luoghi insicuri" e pertanto i dispositivi portatili non devono essere lasciati incustoditi all'interno di essi, anche nel caso in cui non siano visibili dall'esterno (ad es. riposti nel bagagliaio).

Nel caso di perdita, smarrimento o furto del dispositivo portatile assegnato, il dipendente deve avvertire immediatamente le strutture competenti (Ufficio Legale, Ufficio Patrimonio e Logistica, Gestione Telematica) e, qualora ne ricorrano le circostanze, deve immediatamente denunciare l'evento alle Forze dell'Ordine e consegnare copia della verbalizzazione.

L'*Istituto* si riserva il diritto di sospendere l'utilizzo di un dispositivo e di richiederne la restituzione qualora non sia più necessario all'esecuzione delle attività del Dipendente in relazione al ruolo ricoperto e alle mansioni assegnate, in presenza di cessazione del rapporto di lavoro o a fronte di un utilizzo non conforme al presente **Regolamento**.

In tutti questi casi è fatto obbligo al Dipendente di procedere alla restituzione del dispositivo assegnato avendo cura di cancellare eventuali dati personali che fossero presenti al suo interno. In ogni caso l'*Istituto* non può essere ritenuto responsabile di eventuali dati o file ad uso personale che i suoi dipendenti possano aver memorizzato sui dispositivi assegnati.

ART. 7 - PC E COMPUTER PORTATILI

L'*Istituto* mette a disposizione dei dipendenti un Personal Computer (fisso o portatile) già predisposto ed opportunamente configurato.

La dotazione hardware e *software* del Personale Computer, fisso o portatile, può variare in funzione del ruolo aziendale e della mansione assegnata al dipendente.

Non è consentito al dipendente di modificare le componenti *hardware* e *software* del proprio PC, fisso o portatile.

Qualora fosse necessario disporre di una dotazione *hardware* e/o *software* differente da quella assegnata, il dipendente deve rivolgersi al proprio **Responsabile** che inoltra la richiesta tramite apposita applicazione di approvvigionamento. Richiesta che seguirà il flusso di approvazione previsto relativamente agli aspetti di opportunità, sicurezza e scelta tecnologica.
Fanno eccezione unicamente i software di service a macchine di laboratorio che gestiscono strumenti di analisi per i quali la variazione di dotazione è in capo al **Responsabile di Reparto**.

Al fine di evitare che il dispositivo elettronico possa essere utilizzato impropriamente da altri soggetti senza che vi sia la possibilità di provarne in seguito l'indebito accesso, il dipendente, qualora non ne preveda l'utilizzo e comunque al termine dell'attività lavorativa, deve provvedere a spegnere il Personal Computer (fisso o portatile) e, nel caso di allontanamento temporaneo, deve provvedere a bloccarne l'accesso tramite la modalità manuale di blocco (*screen saver*), presente sul PC stesso.

Qualora il Dipendente utilizzi il PC portatile per operare da remoto (es. in *smartworking)*, deve adeguarsi alle disposizioni che gli verranno di volta in volta impartite.

Al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro *virus, spyware*, *malware*, ecc., il personale tecnico con qualifica di "*Amministratore di Sistema*" può avere la necessità di collegarsi anche da remoto al PC (fisso o portatile) a seguito di specifica richiesta del Dipendente che deve autorizzarlo. Comunque, in caso di oggettiva necessità – e cioè a seguito di problematiche tecniche, rilevate e rischiose, rispetto alla rete e/o ai sistemi informativi aziendali – il personale tecnico incaricato, autorizzato dal **Responsabile Gestione Telematica**, potrà intervenire direttamente, al fine di non pregiudicare la necessaria immediatezza ed efficacia dell'intervento, fornendo al dipendente tempestiva comunicazione dell'avvenuto accesso.

ART. 8 – LICENZE SOFTWARE

Qualunque applicativo software venga utilizzato all'interno delle strutture dell'*Istituto* deve essere accompagnato da regolare licenza d'uso.

È fatto tassativo divieto al dipendente che utilizza computer aziendali di scaricare dalla rete Internet qualsiasi software non autorizzato o installare sulle macchine stesse software privi di licenza d'uso provenienti dall'esterno.

È altresì vietata la riproduzione o la duplicazione di programmi informatici o di una parte di essi se sviluppati all'interno dell'Istituto.

Si evidenzia che la normativa sulla tutela dei brevetti industriali e del diritto d'autore impone che nel Personal Computer (fisso o portatile) sia presente esclusivamente software

regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore. Le violazioni possono comportare il sorgere di una responsabilità amministrativa a carico del Dipendente e dell'*Istituto* e possono essere sanzionate anche penalmente nei confronti del trasgressore.

ART. 9 - SUPPORTI RIMOVIBILI

Il dipendente può utilizzare supporti rimovibili aziendali (chiavette USB, hard-disk esterni, …) in funzione dell'attività svolta, previa autorizzazione del proprio **Responsabile**.

Qualora autorizzato all'utilizzo di supporti rimovibili aziendali deve rispettare le seguenti prescrizioni:

- è responsabile della custodia dei supporti rimovibili a lui assegnati e dei dati aziendali in essi contenuti e deve trattarli con particolare attenzione onde evitare che il loro contenuto possa essere reso disponibile a terzi o possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato;
- può utilizzarli solo se collegati ad un dispositivo aziendale;
- non può utilizzarli per uso personale o cederli a terzi.

Nel caso di supporti rimovibili trasmessi da una controparte il Dipendente, prima dell'utilizzo, deve provvedere alla sua verifica mediante il programma antivirus. Qualora venisse rilevato un virus, deve rimuovere il dispositivo e segnalare l'evento al **Reparto Gestione Telematica** (vedi *Capo V - Gestione degli Incidenti di Sicurezza IT*) per gli interventi del caso.

E' vietato l'utilizzo di supporti rimovibili personali quali chiavette USB, hard-disk esterni, …

ART. 10 - PROTEZIONE DA VIRUS E DA MALWARE

Il sistema informatico aziendale è protetto da *software antivirus* mantenuto periodicamente aggiornato.

È fatto assoluto divieto di disinstallare, modificare le impostazioni o disattivare anche solo temporaneamente l'antivirus, in quanto pericoloso per il proprio PC e per l'intera Rete Aziendale.

Pur in presenza di un antivirus aggiornato, il Dipendente deve comunque mettere in atto comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro *software* aggressivo (*malware*).

Nel caso in cui il *software* antivirus rilevi la presenza di un virus, il Dipendente deve sospendere immediatamente ogni elaborazione in corso, scollegare il PC dalla rete, evitando ove possibile di spegnerlo, nonché segnalare prontamente l'evento al **Reparto Gestione Telematica** (vedi *Capo V - Gestione degli Incidenti di Sicurezza IT*).

ART. 11 - STRUMENTI DI FONIA MOBILE E/O DI CONNETTIVITÀ IN MOBILITÀ

L'*Istituto* mette a disposizione, a seconda del ruolo o della funzione del singolo utente, impianti di telefonia fissa e mobile, nonché dispositivi quali smartphone e tablet.

L'utilizzo di tali dispositivi risponde alle regole che di seguito si riportano:

a. devono essere dotati di password di sicurezza (ad esempio, il codice pin del dispositivo) che ne impedisca l'utilizzo da parte di soggetti non autorizzati;
b. in caso di furto o smarrimento l'*Istituto* si riserva la facoltà di attuare la procedura di remote-wipe (cancellazione da remoto di tutti i dati sul dispositivo), rendendo il dispositivo inutilizzabile e i dati in esso contenuti irrecuperabili;
c. in ogni caso, al fine di evitare e/o ridurre al minimo la possibile circolazione di dati personali sull'apparecchio, si ricorda agli assegnatari di cancellare tutti i dati eventualmente presenti prima di consegnare il cellulare agli uffici competenti per la restituzione o la riparazione.

ART. 12 - STAMPANTI, FOTOCOPIATRICI E FAX

Nell'utilizzo di stampanti condivise, fotocopiatrici e fax, è fatto obbligo attenersi alle seguenti regole:

a. non lasciare le stampe incustodite e ritirare immediatamente le copie in caso di documenti contenenti dati personali o informazioni riservate; ciò al fine di evitare che persone non autorizzate possano venirne a conoscenza;
b. evitare l'utilizzo dei fax per l'invio di documenti che hanno natura strettamente confidenziale. Nei casi in cui questo sia necessario, si deve preventivamente avvisare il destinatario, in modo da ridurre il rischio che persone non autorizzate possano venirne a conoscenza e successivamente chiedere la conferma telefonica di avvenuta ricezione.

ART. 13 - DISPOSITIVI ELETTRONICI PERSONALI

È vietato l'uso aziendale di dispositivi personali (PC, smartphone, tablet, chiavette USB, etc.), salvo specifica autorizzazione da parte del **Responsabile Sicurezza IT**, su richiesta del proprio **Responsabile.**

Qualora l'uso venga autorizzato, il **Reparto Gestione Telematica** disporrà opportuna assistenza all'utente per la configurazione del dispositivo e fornirà le adeguate istruzioni per la configurazione e l'utilizzo dello stesso per le finalità in ambito aziendale.

Capo II

POSTA ELETTRONICA

ART. 14 - FINALITÀ DELL'UTILIZZO DELLA POSTA ELETTRONICA

La casella di posta elettronica (*casella e-mail*) assegnata al Dipendente è uno strumento di lavoro di proprietà aziendale e viene concessa in uso al Dipendente al fine di un più proficuo svolgimento della prestazione lavorativa, nel rispetto di quanto descritto all'art. 3.

Tutte le caselle di posta elettronica messe a disposizione dall'*Istituto*, anche se di tipo individuale, sono di esclusiva proprietà dell'*Istituto*, che deve essere considerato rispettivamente come mittente o destinatario dei messaggi in entrata ed in uscita, il cui contenuto può legittimamente apprendere.

ART. 15 – DIVIETI E RACCOMANDAZIONI

Il Dipendente assegnatario di una casella di posta elettronica è responsabile del corretto utilizzo della stessa.

È fatto divieto di utilizzare la casella di posta elettronica aziendale per motivi diversi da quelli strettamente legati all'attività lavorativa.

Sulla base delle Linee-guida del Garante per la protezione dei dati personali, per ogni e-mail inviata all'esterno è obbligatorio inserire come nota finale, allegata in automatico, l'informativa (disclaimer) appositamente predisposta a fini Privacy.

Nell'inviare o ricevere una e-mail è obbligatorio attenersi alle seguenti regole:

a. non inviare messaggi con contenuto o mittente falsi o alterati;
b. non spedire, ridistribuire o rispondere a messaggi diffamatori, calunniosi, minacciosi, ingannevoli;
c. non inviare messaggi con allegati o link a siti considerati non pertinenti;
d. non aprire gli allegati o cliccare sui link di e-mail ricevute da persone sconosciute o riguardanti un oggetto sospetto al fine di limitare il rischio di attivazione di virus o altri codici maligni;
e. non partecipare alle cosiddette lettere a catena;
f. non comunicare il proprio identificativo per l'invio della posta all'esterno, se non per motivi strettamente inerenti alla propria attività professionale.

Al fine di soddisfare esigenze di sicurezza, è vietato:

a. abilitare programmi o macro ricevuti tramite posta elettronica dall'esterno;
b. inviare all'esterno tramite posta elettronica le proprie credenziali di autenticazione, le configurazioni della rete interna, gli indirizzi e i nomi dei sistemi informatici;
c. fornire all'esterno, in particolare a seguito di richiesta dati pervenuta tramite e-mail, informazioni riservate, quali codici di identificazione, numeri di carte di credito, codici dispositivi per l'home banking.

Il Dipendente, nel caso di ricezione di una mail da un mittente conosciuto che richieda però

comportamenti difformi da quanto previsto dalle procedure abituali, deve sempre chiedere conferma al mittente utilizzando un canale di comunicazione differente (ad es. telefono, colloquio diretto, …), in quanto è possibile che la richiesta sia connessa a un furto di identità.

Qualora il Dipendente sia autorizzato all'utilizzo delle caselle di PEC (Posta Elettronica Certificata) aziendali, deve adeguarsi alle disposizioni che gli verranno comunicate sullo specifico tema, che si aggiungono ed integrano il presente **Regolamento.**

ART. 16 - CONTINUITÀ DEL SERVIZIO E PROCEDURA DI EMERGENZA PER L'ACCESSO ALLA POSTA ELETTRONICA DEL LAVORATORE ASSENTE

In caso di assenze programmate (ad es. per ferie), il dipendente può configurare la propria *casella email* affinché invii automaticamente un messaggio di risposta che dichiari la propria assenza ed eventualmente proponga un altro indirizzo e-mail a cui inviare comunicazioni urgenti (c.d. "messaggio di cortesia"). In nessun caso dovrà impostare inoltri automatici ad indirizzi *e-mail* di altre persone senza un accordo preventivo.

Al fine di garantire la continuità dell'attività lavorativa e la sicurezza del sistema, nell'ipotesi in cui il lavoratore sia impossibilitato ad accedere ai servizi di posta elettronica (es: in caso di malattia, di assenza improvvisa o prolungata o per improrogabili necessità legate all'attività lavorativa), l'*Istituto* si riserva la possibilità di accedere a messaggi di posta elettronica ritenuti rilevanti ai fini lavorativi qualora ricorrano le seguenti condizioni:

a. nei soli casi in cui vi sia un'esigenza indispensabile e indifferibile;
b. solo per il tempo strettamente necessario al reperimento delle informazioni richieste.

L'attività, nel rispetto della normativa vigente, è indirizzata dalla "*Procedura per la Forzatura di Utenze e Caselle Email*" che, in particolare, prevede l'avviso al dipendente e la tracciatura delle autorizzazioni date e delle attività svolte.

In caso di interruzione del rapporto di lavoro, le credenziali di accesso alla casella di posta elettronica vengono tempestivamente disattivate e l'indirizzo di posta elettronica verrà eliminato dopo 30 giorni. Dalla data di interruzione il personale del **Reparto Gestione Telematica** provvederà ad impostare una risposta automatica che, nel respingere il messaggio, informa il mittente sulla cessazione del rapporto di lavoro del destinatario invitandolo a riproporre la mail ad un altro specifico indirizzo di posta.

ART. 17 - CONTROLLI PREVENTIVI E SUCCESSIVI

I messaggi ricevuti dall'esterno e inviati all'esterno della rete sono sottoposti alla scansione antivirus e antispamming, con eventuale cancellazione degli allegati considerati pericolosi e la rimozione preventiva delle e-mail considerate spam.

Il sistema può bloccare delle email legittime (*antispam*) e per questo il Dipendente è tenuto a prestare attenzione agli avvisi inoltrati dall'antispam. Nel caso riceva ripetutamente messaggi di spam non intercettati dal sistema antispam, deve segnalare la situazione al **Reparto Gestione Telematica** per un aggiornamento dei relativi filtri.

Capo III

RETE INTERNET

ART. 18 - REGOLE DI UTILIZZO

Al Dipendente può essere messa a disposizione la "*navigazione Internet*" per lo svolgimento dell'attività lavorativa

L'*Istituto* è consapevole che la rete Internet costituisce ormai parte essenziale della vita quotidiana e ammette, quindi, un utilizzo sporadico e limitato della navigazione per fini personali, purché avvenga fuori dell'orario lavorativo e non esponga i sistemi informatici aziendali ad alcun rischio.

La navigazione, al fine di ricerca di informazioni, deve limitare al minimo l'ingombro della banda di connessione, conseguentemente le dimensioni dei file scaricati dovranno essere le più contenute possibili.

ART. 19 - DIVIETI

Sono vietate in modo tassativo le seguenti attività:

a. navigazione in Internet in orario lavorativo per motivi diversi da quelli strettamente legati all'attività;
b. utilizzo di modem privati per il collegamento alla rete se non previa autorizzazione;
c. download/upload di software o file musicali, film o immagini non autorizzato o comunque non legato all'attività lavorativa.

ART. 20 - CONTROLLI PREVENTIVI

L'*Istituto* è dotato di un sistema di protezione perimetrale che prevede strumenti di antivirus, antispam, web filtering e IDPS, al fine di prevenire determinate operazioni quali l'accesso a determinati siti (inseriti ad esempio in una black list) e il download di file o software considerati dannosi.

ART. 21 - CONTROLLI SUCCESSIVI

Il sistema di protezione perimetrale adottato dall'Istituto consente di monitorare il traffico relativo alla navigazione Internet e ha la possibilità di raccogliere dati, per reparto o per postazione, relativi ai siti visitati, ai siti cui non è stato consentito l'accesso, ai volumi di traffico, al numero di accessi e al tempo di permanenza su ogni pagina.

I log di navigazione, relativi a tutto il traffico web in entrata e in uscita, sono conservati per un periodo non superiore a sei mesi, eventualmente prolungabile in relazione a:

a. esigenze tecniche o di sicurezza del tutto particolari;
b. indispensabilità del dato rispetto all'esercizio di un diritto in sede giudiziaria;
c. obblighi di custodia e consegna imposti dall'Autorità giudiziaria o dalla Polizia giudiziaria.

L'accesso ai *log* suddetti avviene esclusivamente nei casi e con le modalità previste dalla "*Procedura per il Controllo della Navigazione Internet*". Tale controllo non è continuativo, ma viene posto in essere solo in presenza di anomalie e viene effettuato inizialmente sulla base di informazioni anonime e aggregate, intervenendo in modo più accurato solo qualora circostanze oggettive e documentate ne giustifichino la necessità, applicando il sistema dei controlli graduali (vedi *Capo VI - Sistema dei controlli*).

Capo IV

SOCIAL MEDIA

ART. 22 - REGOLE DI UTILIZZO

L'utilizzo a fini informativi e/o promozionali dei Social Media effettuato a nome dell'*Istituto* (es. Facebook, Twitter, Instagram, Blog, Forum, ecc.) viene gestito e organizzato esclusivamente attraverso specifiche autorizzazioni, direttive e istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli Dipendenti.

ART. 23 - DIVIETI

Qualora il Dipendente, sui propri profili privati, scegliesse di rendere noto che lavora per l'*Istituto*, è tenuto a specificare che le opinioni espresse hanno carattere personale e non impegnano in alcun modo la responsabilità dell'*Istituto.*

Il Dipendente sui propri profili privati non può diffondere contenuti o eventi aziendali che non siano già stati precedentemente segnalati sui canali social ufficiali o comunque già presenti sul sito pubblico dell'*Istituto* o su un altro sito pubblico istituzionale di riferimento.

Il Dipendente non può divulgare attraverso i Social Media informazioni aziendali riservate, quali ad esempio comunicazioni interne, informazioni di terze parti (ad esempio partner, istituzioni, clienti, ecc.) di cui è a conoscenza o informazioni su attività lavorative, servizi, progetti e documenti prima che queste siano diventate di dominio pubblico.

Capo V

GESTIONE DEGLI INCIDENTI DI SICUREZZA IT

ART. 24 - PRESCRIZIONI

Gli **Incidenti di Sicurezza IT**, intesi come eventi che possano compromettere la Sicurezza Aziendale (in particolare eventi di *CyberSecurity*), si verificano sempre più frequentemente e l'*Istituto* è consapevole della minaccia.

Per affrontare adeguatamente tali eventi è necessario che i Dipendenti assumano un atteggiamento responsabile e consapevole della presenza di potenziali rischi e delle azioni necessarie per evitarli.

Una risposta efficace prevede una reazione rapida e per questo è necessario riconoscere tempestivamente un potenziale **incidente di sicurezza IT**, come ad esempio:

- la segnalazione della presenza di un possibile virus;
- la rilevazione di una situazione insolita o inattesa (ad es. una password disabilitata senza un motivo apparente);
- la rilevazione di comportamenti insoliti del PC (ad es. continui riavvii);
- la richiesta insistente di informazioni personali senza un valido motivo.

È responsabilità di ciascun Dipendente, qualora venga a conoscenza di un potenziale Incidente di Sicurezza IT, effettuare prontamente una segnalazione al **Reparto Gestione Telematica** secondo le modalità specificamente previste.

L'*Istituto* programma periodici interventi di formazione per sensibilizzare i Dipendenti sulle minacce di sicurezza e per fornire le indicazioni da seguire per fronteggiarle.
I Dipendenti devono prestare la massima attenzione al tema, chiedendo chiarimenti ove ritenuto necessario, e devono adeguare i comportamenti a quanto richiesto.

Capo VI

SISTEMA DEI CONTROLLI

ART. 25 - FINALITÀ E MODALITA' DI ESECUZIONE

Si ricorda che sugli strumenti elettronici utilizzati, sui server acceduti e sui firewall rimangono sempre tracce delle attività svolte (*Log*).

L'*Istituto*, nel rispetto del divieto di utilizzo di strumenti tecnologici preordinati al controllo dell'attività lavorativa dei Dipendenti, assicura che strumenti tecnologici di controllo potranno essere installati, se del caso, esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e/o per la tutela del patrimonio, e per tutte le finalità previste dal rapporto di lavoro e previa idonea informativa all'interessato, e, ove necessario, tramite accordo sindacale o autorizzazione dell'Ispettorato del Lavoro, ai sensi dell'art. 4, comma 1, legge n. 300/1970 e successive modificazioni.

Eventuali controlli, che in nessun caso saranno prolungati, costanti o indiscriminati, potranno avvenire con modalità di *controlli graduali*, come di seguito definito:

A. **Controlli generalizzati**: in caso di anomalie o malfunzionamenti, il personale incaricato effettuerà, mediante l'ausilio dei sistemi installati, controlli anonimi che si concluderanno con avvisi generalizzati diretti a tutto il personale. I suddetti avvisi evidenzieranno i comportamenti rilevati non conformi alle prescrizioni e inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite.

B. **Controlli su base individuale**: in caso di persistenza dell'anomalia, successivamente all'invio dell'avviso generalizzato, il personale incaricato potrà effettuare interventi mirati seguendo comunque procedure definite allo scopo.

Controlli su base individuale potranno comunque venire effettuati in via eccezionale e tassativa, oltre che nell'ipotesi sopra menzionata, anche ove ricorra una o più delle seguenti ipotesi**:**

- quando venga presentata una specifica richiesta di informazioni da parte dell'Autorità giudiziaria;
- quando si verifichi un evento dannoso o una situazione di pericolo che richiedano un immediato e necessario intervento.

I dati raccolti dai predetti controlli potranno essere utilizzati per tutte le finalità connesse al rapporto di lavoro, nel rispetto della normativa *Privacy*, dello Statuto dei Lavoratori e del contratto di lavoro vigente.

Titolo IV

DISPOSIZIONI FINALI

ART. 26 - SANZIONI

È fatto obbligo ai Dipendenti di adeguarsi a quanto richiesto dal presente **Regolamento**, in quanto ogni comportamento non conforme ad esso espone l'*Istituto* ad eventuali danni patrimoniali e/o penali che possono compromettere la sicurezza e l'immagine dell'*Istituto,* risultando così perseguibili nelle sedi proprie (disciplinare, civile e/o penale).

Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile con provvedimenti disciplinari e risarcitori previsti dal contratto collettivo di lavoro applicato al rapporto di lavoro tra dipendente e *Istituto*, nonché con tutte le azioni civili e penali consentite.

Ai sensi dell'art.4, comma 4, legge n. 300/1970 le informazioni raccolte attraverso l'uso degli strumenti informatici sopra descritti sono utilizzabili a tutti i fini connessi al rapporto di lavoro.

ART. 27 - AGGIORNAMENTO E REVISIONE

Il presente **Regolamento** è soggetto a revisione periodica, almeno annuale e comunque in caso di modifiche dei processi e delle *policy* aziendali.

La versione aggiornata del **Regolamento** è disponibile nella Sezione Regolamenti Interni sulla Bacheca presente sulla Intranet aziendale.

A fronte di modifiche del **Regolamento** viene inviata a tutti i Dipendenti una specifica comunicazione (*e-mail*) di avviso.

ART. 28 - ENTRATA IN VIGORE E DIFFUSIONE

Il presente **Regolamento di Sicurezza Informatica per il personale interno** entra in vigore a partire dalla data di approvazione sotto riportata.

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

Il presente **Regolamento di Sicurezza Informatica per il personale interno** viene comunicato ai singoli soggetti interessati, viene esposto in bacheca, reso disponibile nella Intranet aziendale e ulteriormente a disposizione del Dipendente a richiesta.

Data di approvazione: 30/06/2023

GLOSSARIO

Sono di seguito elencate alcune definizioni ricorrenti nel presente Regolamento, inerenti al trattamento dei dati personali ovvero all'informatica.

Autenticazione informatica: "L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità".

Credenziali di autenticazione: I dati ed i dispositivi in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica (username e password).

Dati giudiziari: Dati idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative, dipendenti da reato e dei relativi carichi pendenti o la qualità di imputato o di indagato, il cui trattamento è ammesso solo se autorizzato da espressa disposizione di legge o provvedimento del Garante, che ne specifichi le finalità, i tipi di dati e le operazioni autorizzate.

Dati sensibili: Dati che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale, nonché i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale.

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

Diffusione: "Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione".

Dispositivi di memoria portatili: per dispositivi di memoria portatili si intendono tutti quei dispositivi che consentono di copiare o archiviare dati, file o documenti esternamente al computer. Sono considerati tali CD-ROM, DVD, chiavi di memoria USB, riproduttori musicali, fotocamere digitali, dischi rigidi esterni, etc.

Dispositivi informatici: si intendono gli strumenti messi a disposizione del personale per svolgere attività lavorativa (personal computer fissi e portatili, stampanti, smartphone, etc.).

IDPS (Intrusion detection and prevention systems)*:* sono dei componenti software attivi sviluppati per incrementare la sicurezza informatica di un sistema informatico, individuando, registrando le informazioni relative e tentando di segnalare e bloccare le attività dannose.

Password: "Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica".

Posta elettronica: per servizio di posta elettronica interno si intende il sistema informatico su cui operano gli indirizzi di posta elettronica (e-mail) aziendali e da cui si possono inviare e ricevere messaggi di posta elettronica sia interni sia da e verso Internet.

Postazione di lavoro: si intende il complesso unitario di PC, notebook, accessori, periferiche e ogni altro device concesso dall'Istituto, in utilizzo all'utente.

Rete internet: per rete Internet si intende la rete mondiale di comunicazioni basata sul protocollo TCP/IP e più specificamente il World Wide Web e l'attività di navigazione all'interno dello stesso.

Software aziendale: qualunque applicativo software utilizzato all'interno della struttura aziendale,

accompagnato da regolare licenza d'uso, finalizzato allo svolgimento di attività lavorative.

Spamming: detto anche fare spam, è l'invio di grandi quantità di messaggi indesiderati, generalmente commerciali.

Trattamento: "Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la 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".

Violazione dei dati personali: "La 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".

Web filtering: definito come "software di controllo dei contenuti", è un componente software progettato per limitare l'accesso a siti web che contengono software dannoso (malware).