CONSIGLIO REGIONALE DELL'ABRUZZO

DISPOSIZIONI, REGOLE DI COMPORTAMENTO E MISURE ORGANIZZATIVE PER IL CORRETTO UTILIZZO DEGLI STRUMENTI DIGITALI E PER LA PREVENZIONE DEI REATI INFORMATICI

Il presente regolamento (di seguito anche Policy) è adottato dal Consiglio regionale dell'Abruzzo (di seguito anche Amministrazione) per disciplinare il corretto comportamento e utilizzo degli strumenti digitali istituzionali al fine di prevenire talune condotte improprie o illecite.

Attraverso la Policy vengono così definite le regole tecniche ed organizzative da applicare e rispettare, nonché quelle per l'utilizzo della posta elettronica e per la navigazione in internet da parte dei Consiglieri, dei dipendenti e dei collaboratori (di seguito anche utilizzatori) nell'ambito dello svolgimento delle loro funzioni/mansioni. La diffusione delle nuove tecnologie informatiche, le maggiori possibilità di interconnessione tra computer e l'aumento di informazioni trattate con strumenti elettronici aumentano, infatti, i rischi legati alla sicurezza e all'integrità delle informazioni, oltre alle conseguenti responsabilità previste dalla normativa vigente in materia.

Pertanto, a seguito dell'adozione della presente Policy, l'Amministrazione auspica che l'utilizzo delle risorse informatiche e telematiche avverrà nell'ambito del generale contesto di diligenza, fedeltà e correttezza e, quindi, che verranno adottate tutte le cautele e le precauzioni necessarie per evitare le possibili conseguenze dannose che un utilizzo non avveduto dei suddetti strumenti può comportare.

La Policy del Consiglio regionale dell'Abruzzo è suddivisa in 13 capitoli:

Nel primo capitolo vengono definite le figure del titolare e del responsabile del trattamento dei dati personali e vengono stabiliti gli obblighi a cui devono attenersi.

Nel secondo capitolo vengono fissate le modalità di diffusione della Policy e della formazione del personale.

Nel terzo capitolo vengono sancite le regole di utilizzo delle postazioni di lavoro e imposti determinati obblighi agli utilizzatori.

Nel quarto capitolo vengono indicate le modalità di gestione degli strumenti informatici affidati agli utilizzatori in caso di assenza o per motivi di urgente necessità.

Nel quinto capitolo vengono illustrate le modalità di gestione delle password e stabiliti determinati obblighi comportamentali.

Nel sesto capitolo vengono fornite agli utilizzatori le raccomandazioni sull'uso corretto della posta elettronica.

Nel settimo capitolo vengono introdotte le modalità di utilizzo della rete internet e le relative azioni non consentite.

Nell'ottavo capitolo vengono illustrate le regole da seguire per il corretto utilizzo dei dispositivi mobili istituzionali come Tablet e Smartphone.

Nel nono capitolo vengono illustrate le regole da seguire per il corretto utilizzo dei Social netwok da parte degli utilizzatori.

Nel decimo capitolo vengono descritti i sistemi di sicurezza installati sui computer dell'Amministrazione che salvaguardano l'accesso ad Internet da parte degli utilizzatori.

Nell'undicesimo decimo capitolo viene trattata la tematica dei Data Breach e vengono fornite ai dipendenti le correlate raccomandazioni.

Nel dodicesimo capitolo vengono illustrati i sistemi di monitoraggio e le modalità di verifica attuate dal Consiglio regionale dell'Abruzzo a fronte di eventuali eventi anomali all'interno dei sistemi informatici, finalizzati unicamente all'accertamento del rispetto delle regole imposte dalla presente Policy.

Nel tredicesimo capitolo vengono stabilite le sanzioni, il relativo sistema disciplinare ed i provvedimenti adottati dal Consiglio regionale dell'Abruzzo in caso di mancata osservanza della Policy.

Sommario

Premessa

La presente Policy descrive le regole tecniche ed organizzative da applicare per garantire il corretto uso degli strumenti informatici, nonché per l'utilizzo della posta elettronica e per la navigazione Internet, installati sulle stazioni di lavoro di proprietà del Consiglio regionale dell'Abruzzo. Inoltre, esso detta disposizioni dirette a prevenire condotte illecite poste in essere attraverso comportamenti idonei a integrare, mediante azioni od omissioni, le fattispecie di reato previste dall'ordinamento in tema di reati informatici. Il documento sarà periodicamente riesaminato ed aggiornato per assicurare che gli obiettivi in esso indicati siano mantenuti ed adeguati rispetto ai mutamenti normativi ed alle nuove minacce informatiche.

Per limitare al massimo la commissione di suddetti reati, occorre sicuramente partire da una responsabilizzazione di tutti i soggetti che ivi lavorano. Per questo motivo, l'Amministrazione predisporrà corsi di formazione interna al fine di fornire a tutti gli utilizzatori elementi che consentiranno di perfezionare la loro conoscenza e sensibilità sulle tematiche inerenti alla gestione del rischio informatico e, comprendere al meglio ciò che si può e ciò che non si deve fare con gli strumenti informatici.

Pertanto, saranno previste sanzioni nei confronti di soggetti che violino in maniera intenzionale i sistemi di controllo o le indicazioni comportamentali fornite.

Proprietà delle attrezzature

I personal computer con relative periferiche (di seguito indicati più brevemente pc), gli accessi Internet, le caselle di posa elettronica, gli spazi Web, le applicazioni accessibili tramite la rete, gli apparecchi di comunicazione (telefoni, cellulari, fax, modem, etc.) concessi in dotazione ai dipendenti (di seguito indicati più brevemente con il termine RISORSE), sono beni di proprietà del Consiglio regionale dell'Abruzzo che, in quanto tali, devono essere utilizzati esclusivamente come strumenti di lavoro per l'attuazione dei compiti istituzionali e non per ragioni private.
Dette risorse sono affidate all'utilizzatore che deve custodirle in modo appropriato e deve tempestivamente informare il Responsabile Sistemi Informativi in caso di un eventuale furto, del loro danneggiamento o smarrimento.
La risorsa è data in uso all'utilizzatore in relazione al ruolo ricoperto e alle mansioni assegnate ed il Responsabile Sistemi Informativi si riserverà il diritto di sospendere l'utilizzo della stessa qualora venga utilizzata in modo improprio, non sia necessaria all'esecuzione delle attività o nel caso in cui termini il rapporto tra l'utilizzatore e l'Amministrazione.
L'uso della risorsa è strettamente personale ed è affidato a ciascuno con l'impegno a non cederla o farla utilizzare a terzi non autorizzati.
Poiché, le suddette attrezzature sono concesse all'utilizzatore come strumenti di lavoro, è severamente vietato conservare o memorizzare sui PC qualsiasi informazione di carattere personale; nel caso in cui il dipendente contravvenisse a tale disposizione, l'Amministrazione declina ogni responsabilità circa la possibile perdita e/o divulgazione di tali dati, obbligando in ogni caso l'utilizzatore ad informare il suo superiore responsabile della presenza di dati personali memorizzati sui computer, della ragione di tale azione, nonché dell'indicazione delle cartelle che contengono sia file di tipo personale che file istituzionali.

1. Responsabile del trattamento dei dati personali e Responsabile della protezione dei dati (DPO)

Il Regolamento UE n. 679/2016 ha previsto l'introduzione di figure, che possono essere o meno nominate dal Titolare, i cui compiti e responsabilità sono qui richiamati affinché siano adeguatamente noti e compresi da parte degli utilizzatori dei sistemi informativi, indipendentemente dal fatto che essi siano stati effettivamente nominati.

Responsabile Esterno del trattamento dei dati personali

Secondo quanto previsto dall'art. 28 del Regolamento UE n. 679/2016 (di seguito anche GDPR), qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a Responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato. Il GDPR stabilisce che il Responsabile del trattamento non ricorra a un altro Responsabile senza previa autorizzazione scritta, specifica o generale, del Titolare del trattamento. Nel caso di autorizzazione scritta generale, il Responsabile del trattamento informa il Titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri Responsabili del trattamento, dando così al Titolare del trattamento l'opportunità di opporsi a tali modifiche. I trattamenti da parte di un Responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il Responsabile del trattamento al Titolare del trattamento e che disciplini la materia e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

a) tratti i dati personali soltanto su istruzione documentata del Titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il Responsabile del trattamento; in tal caso, il Responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

c) adotti tutte le misure richieste ai sensi dell'articolo 32 del GDPR;

d) rispetti le condizioni imposte dal GDPR per ricorrere a un altro Responsabile del trattamento;

e) tenendo conto della natura del trattamento, assista il Titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui all'art. 15 e ss. del GDPR;

f) assista il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR (pseudonimizzazione e cifratura dati; capacità di assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; una procedura per testare, verificare e valutare, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento; l'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 del GDPR può essere utilizzata come elemento per dimostrare la conformità ai requisiti previsti dal GDPR; notifica di una violazione dei dati personali all'autorità di controllo; comunicazione di una violazione dei dati personali all'interessato;)

g) su scelta del Titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;

h) metta a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

Con riguardo alla lettera h), il Responsabile del trattamento informa immediatamente il Titolare del trattamento qualora, a suo parere, un'istruzione violi il GDPR o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

Quando un Responsabile del trattamento ricorre a un altro Responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del Titolare del trattamento, su tale altro Responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il Titolare del trattamento e il Responsabile del trattamento, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR. Qualora l'altro Responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile iniziale conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro Responsabile. L'adesione da parte del Responsabile del trattamento a un codice di condotta approvato di cui all'articolo 40 del GDPR o a un meccanismo di certificazione approvato di cui all'articolo 42 del GDPR può essere utilizzata come elemento per dimostrare le garanzie previste. Fatti salvi gli articoli 82, 83 e 84 del GDPR di disciplina e responsabilità delle sanzioni amministrative e pecuniarie inflitte nell'ipotesi di violazione del GDPR, se un Responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un Titolare del trattamento in questione.

Responsabile della protezione dei dati (RDP/DPO)

Il Titolare del trattamento designa un Responsabile della protezione dei dati (di seguito anche RDP/DPO) ogniqualvolta:

a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

b) le attività principali del Titolare del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;

c) le attività principali del Titolare del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10 del GDPR.

Il Responsabile della protezione dei dati (DPO) è designato in funzione delle qualità professionali, in ragione della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati e della capacità di assolvere i compiti di cui all'articolo 39 del GDPR. Il Titolare del trattamento si assicura che il Responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. Inoltre, sostiene il DPO nell'esecuzione dei compiti di cui all'articolo 39 sopra richiamato, fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali, ai trattamenti e per mantenere la propria conoscenza specialistica.

Il DPO è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Egli effettua il trattamento stesso, attenendosi alle istruzioni impartite dal Titolare dei dati il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle istruzioni impartite.

Pertanto, a seguito di formale nomina scritta da parte del Titolare, il DPO designato si obbliga a:

- eseguire esclusivamente operazioni di trattamento funzionali alle mansioni ad esso attribuite. Qualora dovesse sorgere la necessità di effettuare trattamenti sui dati personali diversi ed eccezionali rispetto a quelli normalmente eseguiti, il Responsabile dovrà darne tempestiva informativa al Titolare del trattamento;
- operare nel continuativo rispetto dei principi di correttezza, liceità, esattezza, pertinenza e completezza del trattamento medesimo;
- mantenere la più completa riservatezza sui dati trattati e sulle tipologie di trattamento effettuate; tale obbligo è da considerarsi pienamente vigente anche nel caso di cessazione del rapporto di impiego e/o comunque di collaborazione;
- verificare periodicamente l'adeguatezza delle misure di sicurezza adottate in relazione ai trattamenti di propria competenza, valutando, se mutamenti dell'attività di trattamento e/o della tipologia di dati trattati non determinino l'adozione di misure di sicurezza diverse e più adeguate ed in tal caso provvedere alla relativa adozione dandone tempestiva comunicazione al Titolare;

- individuare e nominare per iscritto i sub Responsabili, (persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile*)* impartendo loro, sempre per iscritto, apposite istruzioni che tengano conto delle misure di sicurezza, prescrivendo che essi abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati. Nel caso di trattamento elettronico dei dati, dovrà inoltre verificare che i singoli sub Responsabili applichino tutte le prescrizioni di sicurezza relative alla custodia delle parole chiave;
- comunicare immediatamente al Titolare del trattamento gli eventuali nuovi trattamenti da intraprendere nel suo settore di competenza, provvedendo alle eventuali e necessarie formalità di legge;
- interagire con i sub Responsabili incaricati di effettuare eventuali verifiche, controlli o ispezioni, evadendo tempestivamente le richieste di informazioni da parte dell'Autorità Garante e dando immediata esecuzione alle eventuali indicazioni che pervengano dalla medesima Autorità;
- garantire agli interessati l'effettivo esercizio dei diritti previsti dal Capo III del GDPR, ovvero, il diritto di accesso ai propri dati personali (origine, finalità, estremi identificativi del titolare e responsabile del trattamento, logica applicata per il trattamento con strumenti informatici), l'aggiornamento, l'integrazione, la cancellazione, la limitazione, la rettifica, la portabilità;
- non divulgare, diffondere, trasmettere e comunicare i dati/documenti informatici di proprietà del Titolare del trattamento nella piena consapevolezza che, i dati/documenti rimarranno sempre e comunque di proprietà esclusiva dello stesso Titolare del trattamento e, pertanto, non potranno essere venduti o ceduti, in tutto o in parte, ad altri soggetti;
- informare e fornire consulenza al Titolare del trattamento, nonché ai dipendenti;
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati;
- cooperare con l'Autorità di controllo;
- fungere da punto di contatto per l'Autorità di controllo tra cui la consultazione preventiva.

2. Formazione/Aggiornamento del personale e diffusione del modello nel contesto istituzionale

Il Consiglio regionale dell'Abruzzo promuove la conoscenza della Policy, dei relativi protocolli interni e dei loro aggiornamenti tra tutti i dipendenti che sono pertanto tenuti a conoscerne il contenuto, ad osservarli e contribuire alla loro attuazione.

Ai fini dell'attuazione della Policy, la formazione del personale potrà essere così articolata:

- informativa in sede di assunzione per i neoassunti o dell'insediamento per i Consiglieri;
- accesso all'intranet aziendale con spazio dedicato all'argomento;
- occasionali e-mail di aggiornamento;
- note informative interne;
- corsi di formazione.

Inoltre, l'Amministrazione promuove la conoscenza e l'osservanza della Policy anche tra i partner commerciali e finanziari, i consulenti, i collaboratori a vario titolo, gli utenti ed i fornitori. A questi verranno pertanto fornite apposite informative sui principi, le politiche e le procedure adottate sulla base della presente Policy, nonché i testi delle clausole contrattuali che, coerentemente a detti principi, politiche e procedure, verranno adottate.

3. Utilizzo delle postazioni di lavoro

Le postazioni di lavoro, siano esse fisse o portatili, sono dotate dei necessari dispositivi (hardware) e programmi (software) tali da consentirne il corretto funzionamento e la continuità operativa. L'installazione, la configurazione e l'aggiornamento dei suddetti strumenti sono di esclusiva competenza del personale specializzato ed espressamente incaricato dall'Amministrazione.

Le informazioni (documenti, dati istituzionali, dati personali, dati sensibili etc.) a seconda del loro grado di importanza e riservatezza devono essere trattate (raccolta, elaborazione, cancellazione, modifica, comunicazione, diffusione, etc.) secondo le apposite indicazioni impartite dall'Amministrazione, e dalla presente policy.
I Responsabili provvedono periodicamente ad effettuare attività di salvataggio dei dati (backup) allo scopo di evitare la perdita degli stessi e garantirne un rapido ripristino.

Inoltre, è vietato:

- compromettere il funzionamento delle apparecchiature informatiche con virus o programmi diretti a danneggiare o interrompere il funzionamento dei server che erogano i servizi di posta elettronica ed accesso ad internet;
- utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o dati informatici;
- distruggere, deteriorare o rendere in tutto o in parte inservibili programmi, informazioni o dati istituzionali;
- installare software non espressamente autorizzati dall'Amministrazione;
- accedere, modificare, cancellare o fare copie per sé o per terzi (si considerano tali anche gli altri utilizzatori) dei dati istituzionali;
- accedere abusivamente (violando i sistemi di sicurezza) ad aree riservate del sistema informatico aziendale;
- salvare file personali sui supporti di memorizzazione della propria postazione di lavoro e della rete locale aziendale;
- installare e/o utilizzare qualsiasi tipo di programma che non sia espressamente autorizzato dal Responsabile Sistemi Informativi, anche per ragioni di lavoro, onde evitare il rischio di infezione di virus informatici e, pertanto, alterare la stabilità del sistema informatico aziendale;
- modificare la configurazione del proprio pc, salvo espressa autorizzazione dell'Amministrazione;
- copiare sui computer istituzionali *file* di provenienza incerta o comunque esterna non attinenti alla propria attività lavorativa;
- utilizzare la posta elettronica per scopi personali, salvo casi eccezionali di comprovata urgenza e necessità;
- disattivare, anche temporaneamente, il sistema antivirus e gli altri sistemi di sicurezza installati sui computer istituzionali;

4. Disponibilità degli strumenti affidati all'utilizzatore

In caso di assenza dell'utilizzatore o per motivi di urgente necessità, al fine di garantire al personale autorizzato l'accesso agli strumenti ed ai dati istituzionali devono essere rispettate le seguenti modalità:

- in caso di assenza dell'utilizzatore è facoltà dell'Amministrazione autorizzare la configurazione del sistema di posta allo scopo di reindirizzare le e-mail del dipendente assente verso altro indirizzo istituzionale, anche utilizzando il meccanismo di *aliasing* (sostituzione dell'indirizzo originario con altro indirizzo istituzionale);
- solo il dirigente responsabile può autorizzare per iscritto un altro soggetto a sostituirsi alla persona assente e ad utilizzare la sua *user-id* ed il relativo profilo di accesso;
- il dirigente responsabile può inoltrare una richiesta scritta e motivata alla struttura competente che fornisce il servizio (Responsabile Sistemi Informativi): con tale atto il dirigente, sotto la propria responsabilità, richiede di procedere alla sostituzione della password di accesso con contestuale notifica scritta al dipendente interessato;
- al rientro dall'assenza, il lavoratore dovrà sostituirla con altra personale, in modo da garantire la segretezza delle credenziali stesse.

5. Gestione delle password

Il sistema informatico del Consiglio regionale dell'Abruzzo prevede modalità di autenticazione e di accesso alle risorse informatiche/telematiche che rispettano i principi di unicità, incedibilità e segretezza stabiliti dalla legge. Pertanto, le informazioni riservate sono protette contro gli accessi da parte di personale non autorizzato e la rete aziendale è difesa da appropriate gestioni dei privilegi.

Quindi, è vietato:

- non utilizzare password di accesso al sistema, alla rete, ed ai programmi, composte da lettere maiuscole e minuscole, da numeri, caratteri speciali e simboli (Es. P4$$w0rd_AziEnd@le);
- astenersi dal cambio periodico delle password (ogni 3 mesi se vengono trattati dati sensibili, ogni 6 mesi negli altri casi) secondo quanto stabilito e comunicato dal Responsabile Sistemi Informativi;
- comunicare le proprie password a soggetti diversi dalla Direzione, dal Responsabile del trattamento dei dati e dal Responsabile Sistemi Informativi incaricato, fatto salvo il caso di condivisione autorizzata di risorse hardware;
- nel momento in cui i lavoratori si assentano temporaneamente dalla postazione di lavoro, lasciare la sessione del computer "aperta" (bastano pochi minuti per trasferire e/o copiare dati riservati su un supporto esterno come ad es. CD, USB, etc.);
- appropriarsi, comunicare o diffondere password altrui.

6. Utilizzo della posta elettronica

La posta elettronica è un mezzo di comunicazione messo a disposizione dell'utilizzatore esclusivamente per consentirgli lo svolgimento della propria attività di istituto. Gli utenti a cui è assegnata la casella/indirizzo di posta sono responsabili del corretto utilizzo della stessa.

Le principali raccomandazioni sull'uso della posta elettronica sono:

- evitare l'invio o la ricezione di messaggi di posta elettronica con oggetto o contenuto estranei all'attività istituzionale;
- evitare l'utilizzo di posta elettronica per motivi privati e/o per attività non inerente l'uso di istituto, nonché per l'adesione alle c.d. "catene di Sant'Antonio", per l'iscrizione a newsletter pubblicitarie e simili o comunque non attinenti con l'attività lavorativa;
- nel caso di ricezione di e-mail insolite o di messaggi provenienti da mittenti sconosciuti che contengono allegati o link sospetti, per non correre il rischio di essere infettati da virus, occorrerà cancellare i messaggi senza aprirli ed avvisare il Responsabile dei sistemi informativi o persona da questi delegata;
- nel caso in cui si debba allegare un documento ad un messaggio inviato all'esterno dell'Amministrazione, è preferibile utilizzare un formato che consenta di proteggere da scrittura il documento stesso così da renderlo non editabile;
- pur essendo previsto dal sistema antivirus presente sul server di posta e sul PC il blocco di messaggi di posta elettronica contenenti allegati infetti da virus, con contestuale collocazione degli stessi in area di quarantena, potrebbe accadere che messaggi con allegati con estensioni pericolose o sospette (ad esempio: .exe, .bat, etc.) riescano a by-passare il suddetto sistema antivirus (ad esempio nell'ipotesi in cui il sistema non riconosca un virus appena creato e diffuso); nel caso occorre che l'utente proceda immediatamente all'eliminazione di tali messaggi, senza aprire o salvare per nessun motivo i file sospetti allegati;
- CRYPTOLOCKER RANSOMWARE: Il *ransomware* è un programma informatico dannoso che infetta un dispositivo (PC, tablet, smartphone) bloccando l'accesso ai contenuti (foto, video, file) e chiedendo un riscatto (in inglese, ransom) per "liberarli". Il suo obiettivo principale è quello di crittografare e rendere illeggibili i file presenti sull'hard disk dei dispositivi. Il ransomware si diffonde soprattutto attraverso messaggi - inviati via e-mail, sms o chat o che appaiono su pagine web e social network - che sembrano provenire da soggetti conosciuti e sicuri. Difatti, chi li riceve è indotto ingannevolmente ad aprire allegati o a cliccare link/banner collegati a software dannosi. Si raccomanda, pertanto, di prestare molta attenzione ai messaggi ricevuti anche se possono sembrare innocui e/o spediti da un mittente di fiducia. Gli allegati e/o i link vanno sempre e comunque trattati con molta cautela: un innocuo file di testo potrebbe essere benissimo un file eseguibile potenzialmente pericoloso per il proprio computer e per il sistema informatico dell'Amministrazione. Nel caso di presunta infezione, contattare immediatamente il Responsabile Sistemi Informativi.

7. Utilizzo di Internet

Internet è uno strumento utilizzato da miliardi di persone nel mondo. Queste non sempre hanno interessi e codici comportamentali adeguati alle politiche dell'Amministrazione e, pertanto, bisogna prestare molta attenzione al trattamento dei dati e delle informazioni istituzionali di cui persone malintenzionate o incaute potrebbero fare un uso improprio.

Il servizio di accesso ad internet deve essere utilizzato rispettando le regole di comportamento sotto elencate, salvo i casi espressamente autorizzati dalle competenti strutture organizzative.

All'utilizzatore che accede ad Internet dalla propria postazione di lavoro si raccomanda:

- in caso di registrazioni sul web a servizi attinenti l'attività istituzionale, bisogna fornire le proprie generalità lavorative esclusivamente quando si è autorizzati; in tal caso è possibile e consigliato richiedere specifica assistenza del referente informatico interno al fine di evitare l'invio di informazioni eccedenti e non pertinenti alla registrazione stessa;
- di non installare sui computer istituzionali software che potrebbero essere utilizzati per la fuga di dati, come il quelli per la condivisione di *file peer-to-peer* (es. eMule e/o *BitTorrent)*, quelli di *cloud-storage* (es. *Dropbox*) e di posta elettronica *in-the-cloud;*
- di non scaricare file e software da e su siti internet, anche gratuiti, se non su espressa autorizzazione dell'Amministrazione;
- di non navigare in siti non pertinenti con lo svolgimento delle mansioni assegnate e, in particolare, è fatto assoluto divieto di accesso a siti che per il loro contenuto o tenore possano, secondo valutazioni in base alla diligenza media, comportare inosservanza o violazione di norme di legge.

In particolare non è consentito utilizzare l'accesso ad Internet per:

- scaricare fotografie o file multimediali in genere (Jpeg, MP3, AVI, MPEG e/o altri tipi di file o programmi per la fruizione di contenuto audio/video/immagini) non strettamente legati ad un uso d'ufficio;
- effettuare tentativi di intrusione sui sistemi interni dell'Amministrazione o di altri soggetti pubblici o privati, anche se non protetti da adeguati sistemi di sicurezza;
- effettuare operazioni o transazioni finanziarie tramite Internet, acquisti via internet e simili; qualora tali operazioni siano necessarie per lo svolgimento dell'attività lavorativa devono essere previamente autorizzate dalle competenti strutture organizzative dell'Amministrazione ed essere eseguite nel rispetto delle normali procedure di acquisto;
- partecipare o iscriversi per motivi non professionali a Forum, chat, bacheche elettroniche, *guestbook*, *mail-list*, o effettuare l'attivazione di servizi RSS, anche utilizzando pseudonimi (nickname);
- effettuare streaming, download o upload da internet di contenuti non necessari ai fini dell'espletamento delle proprie mansioni/funzioni.

8. Utilizzo dei dispositivi mobili: Smartphone e Tablet

Oggi, i dispositivi mobili, rappresentano un rischio significativo alla sicurezza di dati e informazioni; se non vengono implementate le corrette applicazioni e procedure di sicurezza, possono infatti diventare un vettore per l'accesso non autorizzato ai dati e alla struttura informatica dell'Amministrazione. L'obiettivo è pertanto quello di evidenziare rischi, adempimenti formali e misure di protezione da tenere in considerazione nel trattamento di dati personali mediante tali dispositivi.

Pertanto, le regole per il corretto utilizzo dei dispositivi mobili istituzionali come Tablet e Smartphone stabilite dall'Amministrazione sono:

- agli utilizzatori è consentito salvare sul o sui dispositivi mobili assegnati solamente i dati essenziali allo svolgimento del proprio lavoro;
- il dispositivo affidato all'utilizzatore non può essere ceduto a colleghi e/o terzi;
- i dispositivi devono essere configurati con una password di accesso (PIN) e un codice di blocco schermo diversi dalle credenziali utilizzate all'interno dell'Amministrazione;
- non è consentito connettere il dispositivo ad un PC privo di protezione antivirus aggiornata e non conforme ai criteri istituzionali stabiliti.
- il responsabile IT della gestione degli strumenti informatici, al fine di prevenire vulnerabilità e difetti, può disporre dei dispositivi secondo necessità, sostituendo, aggiornando, rimuovendo o adeguando in tutto o in parte le componenti hardware e/o software di cui essi si compongono;
- non è consentita l'installazione di programmi e applicazioni diversi da quelli autorizzati e installati dall'Amministrazione;
- l'utilizzatore che abbia necessità di apportare modifiche software o hardware al dispositivo in dotazione, installando nuovi programmi o applicazioni, deve farne preventiva richiesta al responsabile IT;
- in caso di malfunzionamento dei dispositivi o dei relativi accessori, l'utilizzatore dovrà consegnare l'apparecchiatura completa al responsabile IT che provvederà alle dovute verifiche e fornirà, se necessario, un apparecchio sostitutivo.
- è proibito sottoporre i dispositivi a *jailbreak* (Apple) o *root* (Android), ossia a procedure che consentono di sbloccare l'accesso e/o modificare tutti i file del sistema operativo di un dispositivo mobile oltre a permettere l'installazione di applicazioni e pacchetti alternativi a quelli ufficiali rilasciati su AppStore e PlayStore;
- non è consentita la riproduzione, la duplicazione, il salvataggio o il download di programmi o file di ogni tipo (testo, immagini, video, audio, eseguibili) in violazione delle norme sul diritto d'autore;
- in caso di furto o smarrimento dei dispositivi, gli utilizzatori hanno l'obbligo di avvisare immediatamente il Responsabile IT;
- l'utilizzatore ha l'obbligo di comunicare prontamente al Responsabile IT ogni sospetto attacco hacking e/o diffusione non autorizzata dei dati contenuti all'interno del dispositivo mobile;
- sui dispositivi verrà installato, a cura del reparto IT, un software di *remote wiping* che permette di cancellare i dati una volta che il dispositivo stesso dovesse cadere in mani sbagliate.

9. Utilizzo dei Social Network

I social network (Facebook, Twitter e altri) sono "piazze virtuali" ossia dei luoghi in cui, via Internet, ci si ritrova, portando con sé e condividendo con altri fotografie, filmati, pensieri, indirizzi di amici e tanto altro. Essi sono lo strumento di condivisione per eccellenza e rappresentano straordinarie forme di comunicazione, anche se comportano dei rischi per la sfera personale degli individui coinvolti. Oggi, lo sviluppo tecnologico spinge i social a integrarsi sempre più con i telefoni cellulari, trasformando le informazioni che pubblichiamo on-line in una sorta di messaggio multiplo, che giunge istantaneamente a tutti i nostri amici e non.

I social network sono strumenti che danno l'impressione di uno spazio personale, o di piccola comunità. Si tratta però di un falso senso di intimità, che può spingere gli utenti ad esporre troppo la propria vita privata e/o lavorativa, a rivelare informazioni strettamente personali, provocando di conseguenza "effetti collaterali", anche a distanza di anni, che non devono essere sottovalutati.

È bene precisare che, quando vengono inseriti dati personali su un social network, se ne perde il controllo. I dati possono essere copiati da tutti i propri contatti e dai componenti dei gruppi ai quali si aderisce, nonché rielaborati, diffusi, anche a distanza di anni. A volte, accettando di iscriversi ad un social network, si concede all'impresa, che gestisce il servizio, la licenza di usare senza limiti di tempo il materiale che viene inserito on-line: foto, messaggi, etc. Se si decide di eliminare il proprio profilo da un social network, spesso viene permesso solo di "disattivarlo" e non di "cancellarlo". I dati e i materiali inseriti on-line, potrebbero essere comunque conservati nei server o negli archivi informatici dell'azienda che offre il servizio. Il valore di queste imprese è strettamente legato anche alla loro capacità di analizzare in dettaglio il profilo, le abitudini e gli interessi dei propri utenti, per poi rivendere le informazioni a chi ne ha bisogno. In conclusione, il miglior difensore della propria privacy siamo noi. Meglio riflettere bene prima di inserire on-line dati che non si vogliono diffondere o che possano essere usati a proprio danno o a danno degli altri.

Il presente documento indica le principali norme di comportamento che gli utilizzatori del Consiglio regionale dell'Abruzzo sono invitati/tenuti ad osservare quando utilizzano i Social Network.

Si raccomanda di:

a) attenersi alle disposizioni del GDPR, nonché alla Policy sulla sicurezza informatica adottata dall'Amministrazione;

b) non effettuare registrazioni di profili utilizzando dati o marchi dell'Amministrazione o di altre aziende con cui l'Amministrazione collabora, salvo i casi in cui si è autorizzati;

c) considerare lo spazio virtuale del social network come spazio pubblico e non privato, in particolare per quanto riguarda il lavoro e le tematiche che attengono l'Amministrazione;

d) qualora l'appartenenza all'Amministrazione sia desumibile dal profilo dell'utente o rilevabile dal contenuto di un intervento, è sempre necessario specificare che le opinioni espresse hanno carattere personale e non impegnano in alcun modo la responsabilità dell'Amministrazione;

e) non divulgare attraverso i social network informazioni riservate, come informazioni interne, informazioni di terze parti (soggetti privati, altri dipendenti, altre società etc.) di cui si è a conoscenza, informazioni su attività lavorative, servizi, progetti e documenti non ancora resi pubblici;

f) garantire la tutela della privacy delle persone; di conseguenza, si raccomanda di non comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi e in genere di collaboratori istituzionali, se non con il preventivo e personale consenso di questi;

g) evitare, salvo i casi in cui si è espressamente autorizzati dal l'Amministrazione, la divulgazione di foto, video, o altro materiale multimediale che ritragga locali, personale, bambini, genitori, etc. e senza che sia stata rilasciata l'esplicita autorizzazione da parte delle persone coinvolte;

h) astenersi dal porre in essere, nei confronti di terzi, verso l'Amministrazione, i colleghi, gli utenti ed i fornitori, attività che possano essere penalmente o civilmente rilevanti (a titolo esemplificativo, sono quindi vietati comportamenti ingiuriosi, diffamatori, denigratori, discriminatori o che configurano molestie). In tal senso, è vivamente auspicato da parte di tutti un comportamento civile e sobrio, in particolar modo in qualunque occasione in cui l'espressione o il contesto in cui essa avviene possa essere collegata all'ambito istituzionale;

i) non pubblicare contenuti che violino il diritto d'autore e non utilizzare marchi registrati senza autorizzazione;

j) segnalare prontamente ai propri responsabili eventuali contenuti presenti sui social network che possano danneggiare la privacy, la reputazione o l'immagine dell'Amministrazione;

k) evitare di collegarsi e/o di "postare" messaggi, foto o altro materiale multimediale dai propri dispositivi privati (pc, tablet, smartphone, etc.) sui social network durante l'orario di lavoro.

10. Blocchi e filtri della navigazione Internet

Nel Consiglio regionale dell'Abruzzo ogni macchina che può accedere a Internet è protetta da un Antivirus e da un Firewall regolarmente aggiornati, infatti, è attivo un meccanismo di controllo e di blocco della navigazione in Internet che interviene:

a) attraverso l'esame di un elenco di parole predefinite, contenuto in una specifica base di dati nell'elaboratore che permette il servizio di navigazione Internet, che siano presenti nelle pagine web richieste dall'utente;

b) attraverso l'esame di indirizzi di siti web (*url*) richiesti dall'utente, con l'esclusione di quelli che sono contenuti con meccanismi identici al punto precedente, in un elenco di "siti vietati" (*black-list*) il cui accesso è interdetto alla navigazione dall'interno dell'Amministrazione.

11. Violazione dei Dati Personali (Data Breach)

Il regolamento europeo della privacy 2016/679 (GDPR) ha introdotto l'obbligo per tutte le organizzazioni di segnalare alcuni tipi di violazioni dei dati personali all'autorità di vigilanza pertinente. Quando prevista, la segnalazione deve avvenire entro 72 ore dalla scoperta della violazione, laddove possibile.

Qualora la violazione possa comportare il rischio elevato di pregiudicare i diritti e le libertà delle persone, è necessario informarne gli Interessati senza indebiti ritardi.

È necessario assicurarsi di disporre di solide procedure di rilevamento delle violazioni, indagini e reporting interno. Ciò faciliterà il processo decisionale sulla necessità o meno di notificare la violazione all'autorità di vigilanza pertinente e alle persone interessate.

È inoltre necessario tenere un registro delle eventuali violazioni dei dati personali, indipendentemente dal fatto che sia necessario notificarle.

Una violazione dei dati personali significa una violazione della sicurezza che porta alla distruzione, perdita, alterazione, divulgazione non autorizzata o illegale di dati personali. Le violazioni possono essere il risultato di cause sia accidentali che deliberate. Una violazione è, quindi, più che una semplice perdita di dati personali.

Una violazione di dati personali può essere causata ad esempio da:

- attacco informatico o accesso ai sistemi, o ai locali, da parte di terzi non autorizzati;
- azione, deliberata o accidentale (o anche derivante da inazione), da parte di un operatore o di un controllore (personale interno);
- invio di dati personali ad un errato destinatario;
- perdita o furto di server, computer o altri dispositivi informatici (notebook, smartphone, chiavette USB, ecc.) contenenti dati personali;
- alterazione dei dati personali avvenuta senza la debita autorizzazione;
- perdita della disponibilità dei dati personali.

Una violazione dei dati personali può essere quindi definita come un problema/violazione di sicurezza che ha influito sulla riservatezza, l'integrità o la disponibilità dei dati personali. In breve, ci sarà una violazione dei dati personali ogni qualvolta i dati personali vengono persi, distrutti, corrotti o divulgati, se qualcuno accede ai dati o li diffonde senza esserne stato autorizzato, se i dati sono resi non più disponibili (ad esempio, quando sono stati crittografati da azioni di ransomware) o sono andati persi o distrutti accidentalmente.

Il GDPR chiarisce che, quando si verifica un problema/violazione di sicurezza, è necessario stabilire rapidamente se si è verificata una violazione dei dati personali e, in tal caso, adottare prontamente le misure necessarie per risolverlo, inclusa, se necessario, la notifica alle autorità di controllo e agli interessati.

Gli utilizzatori dell'Amministrazione devono informare tempestivamente il DPO, o la persona appositamente delegata, di qualsiasi violazione certa o presunta di cui sono venuti a conoscenza, utilizzando i seguenti canali: e-mail rpd@crabruzzo.it.

12. Monitoraggio e verifiche

Per la tutela del proprio patrimonio informativo, per esigenze organizzative/produttive, per la sicurezza dal lavoro e in ottemperanza a quanto previsto dal D.Lgs. 151/2015 relativo al controllo a distanza dei lavoratori, al fine di garantire un corretto/lecito utilizzo degli strumenti informatici impiegati dagli utilizzatori nello svolgimento delle loro mansioni/funzioni, i sistemi informatici dell'Amministrazione sono dotati di software di *LOGGING* (sistema di memorizzazione di tutte le operazioni che sono considerate critiche per l'integrità del sistema informatico aziendale e di verifica dei tentativi di accesso al sistema stesso, autorizzati e non) e di *MONITORING* (monitoraggio), nei limiti consentiti dalla legge.

L'Amministrazione si riserva la possibilità di condurre attività di verifica degli accessi e delle presenze, del traffico (ma non sui contenuti) e-mail in entrata e in uscita dalle singole postazioni dei dipendenti e sul traffico Internet (anche in questo caso è prevista unicamente un'analisi quantitativa).

Si sottolinea, che tali verifiche, ove effettuate, sono finalizzate unicamente all'accertamento del rispetto delle regole di utilizzo dei dispositivi, della posta elettronica e dei servizi internet istituzionali.

L'accesso e l'analisi dei dati relativi al traffico e-mail ed internet è effettuato dal Responsabile Sistemi Informativi che ha ricevuto espressa autorizzazione allo svolgimento di tale attività.

Il trattamento dei dati contenuti nei *log* può avvenire esclusivamente in forma anonima in modo tale da precludere l'identificazione degli utenti e/o delle loro attività.

I dati anonimi aggregati, riferibili all'intera struttura o a sue aree, sono a disposizione dell'Amministrazione per le valutazioni di competenza, e riguardano:

- per ciascun sito web visitato, le seguenti informazioni: il numero di utenti che lo visitano, il tempo totale di connessione, il numero delle relative pagine richieste e la quantità dei dati scaricati;
- per ciascuna stazione abilitata alla navigazione Internet, le seguenti informazioni: il numero di siti visitati, data e ora delle richieste, la quantità totale di dati scaricati.

L'identificazione dell'utente può avvenire attraverso l'incrocio di più informazioni contenute nei log e negli archivi.

Tali dati personali, possono essere trattati in via eccezionale e tassativamente nelle seguenti ipotesi:

- se richiesti da organi di polizia su segnalazione dell'autorità giudiziaria;
- se richiesti dal Responsabile Sistemi Informativi, anche su segnalazione di un responsabile dell'area con personale assegnato, quando si verifichi un evento dannoso o una situazione di pericolo che richieda un immediato intervento;
- se richiesti dal Responsabile Sistemi Informativi, anche su segnalazione di un responsabile dell'area con personale assegnato, limitatamente al caso di utilizzo anomalo degli strumenti da parte di uno o più utenti di una specifica struttura organizzativa.

È opportuno precisare che, ai sensi della L.48/2008 (Legge di ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica dove sono state delineate definizioni comuni di reato informatico e previsti poteri comuni e di cooperazione nelle indagini) e del D.Lgs. 231/2001, l'Amministrazione ed i propri dipendenti, sono responsabili per la commissione dei seguenti reati informatici:

- falsità in un documento informatico (art. 491-bis c.p.);
- accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.);
- detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.);
- diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.);
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.);
- installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 615-quinquies c.p.);
- danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.);

- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.);
- danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.);
- danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.);
- frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.).

Per questo motivo, i dati contenuti nei *LOG* di sistema sono conservati dall'Amministrazione per finalità organizzative e di sicurezza, solitamente per un periodo non superiore a sei (6) mesi e, successivamente, cancellati attraverso procedure automatiche.

I dati relativi alla navigazione Internet sono utilizzati per garantire la sicurezza del sistema, per verificare la presenza di eventuali abusi, per la ricerca di possibili errori, e/o per analisi di tipo statistico.

Come già precisato, si sottolinea, che tali dati non sono utilizzati per effettuare controlli diretti sull'attività lavorativa.

Nel caso in cui le attività di verifica rilevino abusi o comportamenti illeciti, saranno eseguiti test più approfonditi al fine di accertare eventuali responsabilità ed irrogare le relative sanzioni.

13. Sanzioni

L'utilizzo delle risorse informatiche per finalità o con modalità difformi a quelle indicate in questo documento, configurano gli estremi della infrazione disciplinare perseguibile ai sensi della vigente normativa nonché delle disposizioni previste dal CCNL e/o accordi istituzionali.

In materia di doveri dei lavoratori, l'art. 58 del CCNL 21 maggio 2018, prevede, in base alla gravità delle mancanze dei lavoratori, diversi provvedimenti disciplinari che vanno dal rimprovero verbale, al rimprovero scritto, alla multa in misura non eccedente l'importo di 4 ore della retribuzione, alla sospensione dal lavoro e dalla retribuzione per un periodo non superiore 6 mesi, fino ad arrivare, in presenza di una giusta causa, al licenziamento disciplinare senza preavviso con trattamento di fine rapporto.

L'Amministrazione si riserva inoltre la facoltà di agire a propria tutela per ottenere il risarcimento dei danni eventualmente provocati dal lavoratore con comportamenti non corretti e/o azioni penali in caso di attività dolose o colpa grave.

Sistema disciplinare e misure in caso di mancata osservanza della Policy

La predisposizione di un adeguato sistema sanzionatorio per la violazione delle prescrizioni contenute nella Policy è condizione essenziale per assicurare l'effettività della Policy stessa.

Al riguardo, infatti, l'articolo 6, comma 2, lettera e) del D.Lgs. 231/2001 prevede che i modelli di organizzazione e gestione devono "*introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello*".

L'applicazione delle sanzioni disciplinari prescinde dall'esito di un eventuale procedimento penale, in quanto le regole di condotta imposte dalla Policy sono assunte dall'Amministrazione in piena autonomia e indipendentemente dalla tipologia di illecito che le violazioni del modello stesso possano determinare.

Sanzioni per i lavoratori dipendenti

I comportamenti tenuti dai lavoratori dipendenti in violazione delle singole regole comportamentali dedotte nel presente Modello sono definiti come illeciti disciplinari.

Con riferimento alle sanzioni irrogabili nei riguardi dei lavoratori dipendenti, esse rientrano tra quelle previste dalla Policy, nel rispetto delle procedure di cui all'articolo 7 dello Statuto dei lavoratori e di eventuali normative speciali applicabili.

In relazione a quanto sopra, la Policy fa riferimento alle categorie di fatti sanzionabili previste dall'apparato sanzionatorio esistente.

Tali categorie descrivono i comportamenti sanzionati, a seconda del rilievo che assumono le singole fattispecie considerate, e le sanzioni in concreto previste per la commissione dei fatti stessi a seconda della loro gravità.

In particolare, si prevede che:

1. incorre nei provvedimenti di RIMPROVERO VERBALE, RIMPROVERO SCRITTO, MULTA E SOSPENSIONE DAL SERVIZIO E DALLA RETRIBUZIONE relativamente alla gravità delle proprie mancanze, il lavoratore che violi colposamente, con minimo grado di negligenza, imprudenza o imperizia le procedure interne previste dalla presente Policy (ad es. che non osservi le procedure prescritte, che ometta di svolgere controlli, ecc.) o adotti, nell'espletamento di attività nelle aree a rischio, un comportamento non conforme alle prescrizioni della Policy stessa, dovendosi ravvisare in tali comportamenti una "non esecuzione degli ordini impartiti dall'Amministrazione" o il mancato rispetto di specifici obblighi previsti dall'art.57 del CCNL del 21 maggio nonché dal Decreto 165/2001 come ad esempio:
   - collaborare con diligenza osservando le norme del CCNL,
   - rispettare il segreto di ufficio,
   - non utilizzare a fini privati le informazioni di cui si disponga per ragioni di ufficio;

2. Incorre, inoltre, nel provvedimento di LICENZIAMENTO SENZA PREAVVISO il lavoratore che adotti nell'espletamento delle attività nelle aree a rischio, un comportamento non conforme alle prescrizioni della presente Policy e diretto in modo univoco al compimento di un reato sanzionato dal D.Lgs. 231/2001, dovendosi ravvisare in tale comportamento un "atto tale da far venire meno la fiducia dell'Amministrazione nei confronti del lavoratore";
3. Incorre, infine, nel provvedimento di LICENZIAMENTO SENZA PREAVVISO il lavoratore che adotti, nell'espletamento delle attività nelle aree a rischio, un comportamento palesemente in violazione delle prescrizioni della presente Policy, tale da determinare la concreta applicazione a carico dell'Amministrazione di misure previste dal citato Decreto legislativo, dovendosi ravvisare nel suddetto comportamento, una condotta tale da provocare "all'Amministrazione grave nocumento morale e/o materiale", nonché da costituire "delitto a termine di legge".

ALLEGATO A

GLOSSARIO DEI TERMINI INFORMATICI E/O TECNICI

Account: Iscrizione registrata su un server e che, tramite l'inserimento di una *user-Id* e di una password, consente l'accesso alla rete e/o ai servizi;

Adobe Acrobat: Programma per la creazione e lettura di documenti in formato PDF;

Alias: attribuire un secondo nome, alternativo, ad una casella esistente appartenente o meno al dominio;

Antivirus: è un software programmato per funzionare su un computer ed atto a prevenire, rilevare ed eventualmente rendere inoffensivi codici dannosi, noti anche come malware, fra i quali virus informatici, *adware, backdoor, BHO, dialer, fraudtool, hijacker, keylogger, LSP, rootkit, spyware, trojan, worm;*

Applicazione: programma che viene eseguito su un computer con lo scopo e il risultato di rendere possibile una o più funzionalità, servizi o strumenti utili e selezionabili su richiesta dall'utente;

Attachment/allegato di posta elettronica: file o documento di qualunque genere agganciato ad un messaggio di posta elettronica per essere inviato.

AVI: (*Audio Video Interleaved*) Formato per file video. I video AVI hanno un'ottima qualità di riproduzione, ma di dimensioni maggiori rispetto ad altri formati video;

Bacheca elettronica: servizio internet che permette di reperire annunci di vario genere come, ad esempio, annunci di lavoro e di compravendita;

Backup: replicazione/copia, su un qualunque supporto di memorizzazione, di materiale informativo archiviato nella memoria dei computer;

Black-list: è un file che può contenere nomi di indirizzi di posta elettronica o di siti web per i quali non viene permesso il traffico Internet;

Catena di sant'Antonio è un sistema per propagare un messaggio inducendo il destinatario a produrne copie da spedire, a propria volta, a nuovi destinatari.

Chat: sistema di comunicazione interattiva in tempo reale tramite Internet;

Client: software usato sul computer-client per accedere alle funzionalità offerte da un server;

Client di posta elettronica: è un programma che consente di gestire la composizione e l'organizzazione di e-mail (o messaggi di posta elettronica) da parte dell'utente del servizio, nonché, la ricezione e la trasmissione da e verso un server di posta;

Cloud: servizio di memorizzazione dati attraverso la rete internet, normalmente accessibili con credenziali utente riservate;

Database: "Base di Dati", è un aggregato di dati organizzato.

Download: azione di ricevere o prelevare da una rete telematica (ad esempio da un sito web) un file, trasferendolo sul disco rigido del computer o su altra periferica dell'utente;

Electronic-mail, posta elettronica: scambio di messaggi e di file attraverso una rete locale o Internet.

Feed-reader/RSS: un *feed-reader* è un programma in grado di effettuare il download di un RSS (Really Simple Syndication, uno dei più popolari formati per la distribuzione di contenuti e informazioni web).

E-commerce: sito internet che consente l'acquisto di prodotti/servizi tramite transazioni informatiche;

Estensione di un file: è una breve stringa di caratteri alfanumerici aggiunti dopo il nome di un file e separati da quest'ultimo da un punto.

.exe: estensione di un file che contiene un codice eseguibile, cioè un programma o un driver di dispositivo.

File: insieme di informazioni conservate su supporti di memorizzazione.

Forum: insieme delle sezioni di discussione in una piattaforma informatica, o una singola sezione, oppure lo stesso software utilizzato per fornire questa struttura;

Firewall: termine inglese che significa letteralmente muro taglia-fuoco; è un componente passivo di difesa perimetrale di una rete informatica che garantisce una protezione in termini di sicurezza informatica della rete stessa;

Guest-book: servizio internet che permette ai visitatori di un sito web di lasciare un commento;

Hardware: in informatica si intende l'insieme dei componenti elettronici e meccanici che costituiscono un computer;

Indirizzo IP: (*Internet-Protocol*) è un numero che identifica univocamente nell'ambito di una singola rete i dispositivi collegati alla rete stessa;

Internet: sistema mondiale di reti interconnesse e basate su tecnologie comuni, al quale ogni rete o computer possono essere connessi stabilmente o attraverso collegamenti temporanei;

Intranet: è una rete aziendale privata che utilizza il protocollo TCP/IP;

Jailbreaking: attività effettuata su un dispositivo (generalmente contro le regole che ne determinano l'utilizzo), al né di permettere un'estensione dei servizi IT disponibili;

Log: registrazione sequenziale e cronologica delle operazioni effettuate, da un utente, un amministratore o automatizzate, man mano che vengono eseguite dal sistema o applicazione; il file o insieme di file su cui tali registrazioni sono memorizzate ed eventualmente accedute in fase di analisi dei dati, detto anche registro eventi;

Mailing list: è un servizio/strumento offerto da una rete di computer verso vari utenti e, costituito da un sistema organizzato per la partecipazione di più persone ad una discussione asincrona o per la distribuzione di informazioni utili agli interessati/iscritti attraverso l'invio di email ad una lista di indirizzi di posta elettronica di utenti iscritti;

MP3: è un algoritmo di compressione audio in grado di ridurre drasticamente la quantità di dati richiesti per memorizzare un suono, rimanendo comunque una riproduzione fedele del file originale non compresso;

MPEG: (Motion Picture Experts Group): è un comitato che stabilisce gli standard digitali per file audio e video;

Network: sistema (o rete) di computer collegati tra di loro per il trasferimento o la condivisione di dati, periferiche e programmi;

Password: Serie di caratteri alfanumerici che costituisce la parola d'ordine per accedere a un computer, a un programma, a una banca dati o a una rete;

pdf: (Portable Document Format) Formato di file molto diffuso che consente di creare documenti protetti da modifiche;

Pen-drive: dispositivo mobile di memorizzazione dati attraverso presa USB;

Quicktime: programma utilizzato per la riproduzione dei filmati video/audio;

Remote banking: servizi automatizzati che consentono ai clienti di collegarsi all'elaboratore della banca presso la quale intrattengono il rapporto di conto corrente. Il cliente può effettuare direttamente una serie di operazioni bancarie o ricevere informazioni in tempo reale;

RFC: (*Request For Comment*) è un documento che riporta informazioni o specifiche riguardanti nuove ricerche, innovazioni e metodologie dell'ambito informatico o, più nello specifico, di Internet;

Scheda di memoria SD: dispositivi hardware rimovibili di piccole dimensioni che consentono di memorizzare informazioni, facilmente installabili/rimovibili dai sistemi (in particolare da smartphone o tablet);

Screensaver: (salvaschermo) è un'applicazione per computer che provoca l'oscuramento dello schermo o la comparsa di un'animazione o di una serie di immagini in successione sullo stesso dopo un periodo programmato di inattività del mouse e della tastiera (non dell'elaboratore in sé), impostabile attraverso un timer. L'uso dei salvaschermi è considerato una delle misure di sicurezza per proteggere la propria postazione di lavoro;

Server: è un componente o sottosistema informatico di elaborazione e gestione del traffico di informazioni che fornisce, a livello logico e fisico, un qualunque tipo di servizio ad altre componenti (tipicamente chiamate clients, cioè clienti) che ne fanno richiesta attraverso una rete di computer, all'interno di un sistema informatico o anche direttamente in locale su un computer;

Signature: è un breve contenuto testuale o multimediale che, per scelta dell'utente, viene posto in coda a messaggi di posta elettronica o post su forum o newsgroup;

SIM (Subscriber Identity Module): particolare Smart card denominata UICC, ma nota informalmente come SIM card, che viene usata nel telefono cellulare per identificare il numero dell'abbonato;

Sistema Operativo: (abbreviato in SO) è un insieme di componenti software che rende operativi apparati e dispositivi informatici;

Sito web: è un insieme di pagine web correlate, ovvero una struttura ipertestuale di documenti che risiede su un server web;

Smartphone: dispositivo che unisce funzionalità tipiche di un telefono cellulare a quelle di un computer e che, normalmente, consente la navigazione internet tramite rete mobile (3G e/o wi-fi);

Social-Network: sito o programma che permette lo scambio di informazioni e contenuti multimediali tra utenti attraverso la rete internet (es: *facebook, linkedin, instagram* ecc.);

Software: programmi e procedure utilizzati per far eseguire al computer un determinato compito.

Stazione di lavoro: anche chiamata postazione; è il personal computer utilizzato per accedere anche ai servizi internet e alla posta elettronica;

Tablet: i *tablet* sono dispositivi assimilabili per componenti hardware e software agli *smartphone*, dai quali si distinguono per dimensioni dello schermo, possibile assenza del modulo telefonico, destinazione d'uso;

User-id: Identificativo univoco dell'utente, da utilizzare associato ad una password;

Url: (Uniform Resource Locator) è una sequenza di caratteri che identifica univocamente l'indirizzo di una risorsa in Internet, ad esempio una pagina web;

Virus: programma pirata che si diffonde attraverso lo scambio di dischetti e le connessioni di rete; causa alterazioni di varia entità nel funzionamento dei computer;

Web: (*World Wide Web*) è uno dei principali servizi di Internet che permette di navigare e usufruire di un insieme vastissimo di contenuti

Wikipedia: servizio internet che permette la consultazione di un'enciclopedia online, multilingue, a contenuto libero, redatta in modo collaborativo da volontari.

Usb: porta standard di connessione dispositivi esterni ad un PC o altra apparecchiatura;

Wi-Fi: connessione di un dispositivo ad una rete tramite onde radio (senza utilizzo di cavi di connessione).