ALLEGATO A) 4

NOMINA AMMINISTRATORE DI SISTEMA

In applicazione del **"*Regolamento Europeo sulla protezione e trattamento dei dati personali*" *REGOLAMENTO UE 2016/679*"** nonché ai sensi del **"Provvedimento del Garante della privacy del 27 novembre 2008** "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*"

Premesso che:

- che le prestazioni da lei effettuate in via ordinaria a favore dell'**AZIENDA DI PROMOZIONE E SVILUPPO TURISTICO DI LIVIGNO S.R.L.** forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza, tenuto conto dell'accertata esistenza da parte nostra circa i suoi requisiti di esperienza, capacità ed affidabilità;
- che le caratteristiche dei trattamenti operati presso l'**AZIENDA DI PROMOZIONE E SVILUPPO TURISTICO DI LIVIGNO S.R.L.** non consentono di usufruire delle semplificazioni normativamente previste per i titolari di alcuni trattamenti effettuati in ambito pubblico e privato esclusivamente a fini amministrativo-contabili, i quali pongono minori rischi per gli interessati (art. 29 D.L. 25 giugno 2008, n. 112, convertito con mod., con l. 6 agosto 2008, n. 133; art. 34 del Codice; Provvedimento Garante del 06 novembre 2008);
- che il Garante considera quale "*amministratore di sistema*" tutte le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti e altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi e ciò anche quando l'amministratore non consulti "*in chiaro*" le informazioni relative ai trattamenti di dati personali,
- che gli amministratori di sistema come sopra intesi sono di regola preposti a operazioni da cui discendono grandi responsabilità ed elevate criticità rispetto alla protezione dei dati personali a cui hanno accesso, rispetto a svariati rischi.

Per effetto della presente nomina, il Titolare del trattamento è l'**AZIENDA DI PROMOZIONE E SVILUPPO TURISTICO DI LIVIGNO S.R.L.,** con sede in Livigno (SO), Via RASIA n. 999 (23041) – codice fiscale/ partita IVA n. 92015260141 - in persona del Sig. **LUCA MORETTI**, nella sua qualità di Presidente del Consiglio di Amministrazione, il quale

NOMINA

Rudy Gurini incaricato con mansioni di "**Amministratore del sistema**" (**AS**) in relazione ai trattamenti di dati personali svolti dalla ns. Società o nell'interesse della stessa.

I dati personali ed i relativi ambiti di trattamento sui quali Lei potrà intervenire direttamente o indirettamente nello svolgimento delle Sue mansioni, sono indicati nel MODELLO ORGANIZZATIVO PRIVACY (MOP) del quale Lei dichiara di avere preso visione.

Specificatamente e limitatamente a tale ambito di operatività autorizzato, i suoi compiti sono identificati come meglio segue:

<table>
<tr><th>COD.</th><th>SI=X</th><th>ATTIVITÀ</th></tr>
<tr><td></td><td></td><td>Misure di sicurezza</td></tr>
<tr><td>1</td><td>x</td><td>implementare e gestire le misure minime e supplementari di sicurezza previste dagli artt. da 31 a 35 del D. Lgs. 196/2003, dal Disciplinare Tecnico Allegato B al D. Lgs. 196/2003 e dai provvedimenti del Garante, in relazione ai trattamenti di dati personali svolti mediante strumenti elettronici, in modo da ridurre al minimo i rischi di alterazione, distruzione e perdita anche accidentale e il rischio di accesso non autorizzato o non consentito.
Provvedere ad ogni successivo loro aggiornamento entro i termini di legge; ciò in coordinamento con il Responsabile privacy eventualmente nominato dalla ns. Società.
Lei confermerà l'avvenuta adozione ed aggiornamento periodico di tali misure al Titolare con cadenza almeno semestrale.</td></tr>
<tr><td>2</td><td>x</td><td>rispettare scrupolosamente le regole tecniche ed organizzative previste nel Documento Programmatico sulla sicurezza aziendale, e in eventuali istruzioni o procedure scritte ed orali impartite dal responsabile privacy o dalla Direzione della ns. Società.</td></tr>
<tr><td>3</td><td>x</td><td>Attuare e aggiornare la gestione del sistema di autenticazione sui i sistemi aziendali, in modo da garantire, tra l'altro:
✓ che ciascun utente per l'accesso ai dai e servizi disponibili sui server e sui PC, possa utilizzare una credenziale di autenticazione, costituita di regola da un codice identificativo personale ("user-id") attribuito dall'Amministratore d Sistema, abbinata ad una parola chiave ("password") univoca e scelta dall'utente stesso al primo utilizzo;
✓ che le credenziali di autenticazione degli utenti non privilegiati per l'accesso a dati personali, siano configurate e gestite in modo tale da rispettare i requisiti stabiliti in materia dal Regolamento sull'utilizzo degli strumenti elettronici aziendali costituente parte integrante del Documento programmatico sulla sicurezza, e i seguenti ulteriori criteri minimi previsti dal D. Lgs. 196/2003:
<table>
<tr><th>azione</th><th>tempo</th><th>mezzo</th><th>compito di</th><th>note</th></tr>
<tr><td>Attivazione password</td><td>Entro la data di assunzione della mansione del singolo incaricato</td><td></td><td>Amministratore di Sistema

(su input della Direzione)</td><td>Io user ID non viene assegnato ad altri incaricati, neppure in tempi diversi</td></tr>
</table>
</td></tr>
</table>

			Prima modifica della password	Al primo accesso al sistema		Singolo incaricato	Otto caratteri, alfanumerici, non agevolmente riconducibile all'interessato
			comunicazione al custode della password modificata	Al momento della modifica della password	in busta chiusa solo per eventuali files word-Excel, altrimenti, la credenziale avviene automaticamente archiviata tramite il software di sistema di gestione password	Singolo incaricato	Solo per files word ed Excel se protettiva password
			scadenza periodica della parola chiave	Ogni 6 mesi	in automatico tramite il software di gestione password	Amministratore di Sistema	
			Disattivazione della password	se non utilizzate da almeno 6 mesi (salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica),	in automatico tramite il software di gestione password	Amministratore di Sistema (su input della Direzione o dell'Ufficio del Personale)	
				in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali	Manuale o automatico		
				Anche prima della scadenza di 6 mesi, in caso di pericolo concreto o temuto alla sicurezza dei dati o dei sistemi			
		Fermo restando il Suo obbligo di individuare ed implementare eventuali caratteristiche di maggior sicurezza nel caso di credenziali di autenticazione destinate alla protezione dell'accesso a dati sensibili o a sistemi operativi, apparecchiature, applicazioni o altri database di particolare criticità per l'operatività aziendale (v. oltre).					
4	**x**	Nel caso la Sua figura non coincida con quella del Custode delle Password, custodire con diligenza le credenziali suddette (salvo le stesse non siano già automaticamente conservate in forma criptata all'interno dei sistemi)					
5	**x**	la definizione, implementazione e gestione, sui sistemi elettronici aziendali, del sistema di autorizzazione (cioè dei profili di accesso agli elaboratori, alle applicazioni ed ai dati, nel far ciò Lei dovrà limitare l'accesso degli utenti ai soli sistemi, alle applicazioni e ai dati strettamente necessari e pertinenti allo svolgimento delle mansioni cui è stato assegnato l'incaricato o il gruppo omogeneo di incaricati Resta inteso che Lei non avrà il potere discrezionale di creazione o di cancellazione degli utenti. La creazione, modifica, cancellazione o disabilitazione totale o parziale dell'utente è autorizzato dal Titolare o dall'Ufficio del Personale.					
6	**x**	la installazione, configurazione e aggiornamento dei programmi "antivirus" e relative definizioni dei virus per gli strumenti informatici indicati in allegato alla presente lettera, in modo tale da garantire l'aggiornamento automatico almeno giornaliero dei programmi e pattern file dei virus;					
7	**x**	la selezione, installazione e il costante e tempestivo aggiornamento di sistemi e programmi "antiintrusione" (firewall) per la rete, in particolare l'aggiornamento del firewall dovrà avvenire non appena lo stesso venga reso disponibile dal fornitore; se questa policy si scontra con l'attività di sistemi cruciali, gli aggiornamenti devono essere apportati non appena possibile.					
8	**x**	la selezione, distribuzione e l'aggiornamento degli aggiornamenti (patch di sicurezza, correzioni, HOTFIX, service pack, ecc.) dei software indicati in allegato alla presente lettera (sistema operativo, software applicativi, software di sicurezza), in conformità alle regole previste dal DPS aziendale tali aggiornamenti devono essere installati non appena disponibili; se questa policy si scontra con l'attività di sistemi cruciali, gli aggiornamenti devono essere apportati non appena possibile.					
9	**x**	il monitoraggio sull'installazione di eventuali programmi e hardware non autorizzati, in conformità alle modalità previste nel DPS aziendale					
10	**x**	la implementazione, configurazione e gestione, a livello di server e/o clients, di idonee procedure di backup dei dati, dei sistemi e delle applicazioni, dati, al fine di evitare la perdita o distruzione dei dati ed assicurare la continuità operativa; ciò dovrà avvenire in conformità alle procedure previste nel ns. DPS, che Lei provvederà a tal fine a mantenere aggiornato per quanto riguarda la formale descrizione delle procedure;					
11	**x**	la configurazione di una adeguata procedura di ripristino dei dati, tale da permettere il ripristino degli stessi in tempi certi compatibili con i diritti degli interessati (tali tempi, nel caso di dati sensibili, non devono essere superiori a sette giorni);					
12	**x**	lo smaltimento sicuro dei supporti rimovibili non più utilizzati (es. hard disk, copie di backup delle banche dati trattate), in modo tale che siano sempre state prima cancellate e rese inintelligibili e non più recuperabili i dati personali in essi registrati.					

13	x	il mantenimento in efficienza delle risorse hardware e software indicate in allegato ala presente lettera, (es. con cui sono trattati i dati e con cui avvengono i collegamenti con le reti pubbliche), affinché risultino sempre accessibili e utilizzabili dagli utenti autorizzati segnalare al Titolare eventuali interventi, incidenti o rilevamenti sui sistemi che potrebbero comportare rischi per la sicurezza dei dati (accessi indebiti, trattamenti non autorizzati, non consentiti o non conformi);
14	x	la sorveglianza circa il corretto comportamento (es. rispetto delle misure di sicurezza informatiche della Società) da parte dei terzi soggetti interni ed esterni cui sia consentito l'accesso (in locale o in remoto) ai sistemi aziendali o ai dati trattati con i sistemi;
15	x	la configurazione del sistema di posta elettronica aziendale, al fine di garantire che in caso di assenze dell'utente di caselle e-mail personali, siano disponibili soluzioni funzionali conformi al Provvedimento Generale del Garante dell01.03.2007; e che l'eventuale monitoraggio della posta elettronica e di Internet avvenga in conformità al Provvedimento Generale testé citato, nel Documento Programmatico sulla sicurezza;
		Misure di sicurezza specifiche sulle modalità di intervento urgente su PC o applicazioni protette da password In caso di prolungata assenza o impedimento dell'incaricato, ove si renda indispensabile e indifferibile intervenire per necessità di operatività e di sicurezza di dati personali o di strumenti elettronici ai quali si possa accedere solo tramite password dell'utente: Lei dovrà: a) assicurare la disponibilità di dati e/o strumenti elettronici, b) garantire la segretezza delle password degli incaricati e c) informare tempestivamente l'incaricato dell'intervento effettuato
		Misure relative all'identificazione dell'Amministratore di Sistema
16	x	predisporre, consegnare alla Titolare e al ns. Responsabile privacy, e aggiornare con cadenza almeno annuale (entro il 31 marzo), il suo curriculum vitae, che indichi i Suoi titoli di studio, le certificazioni professionali, le esperienze professionali, i corsi di formazione tecnica svolti. Il CV deve essere datato e da Lei sottoscritto. L'indicazione dei percorsi formativi svolti, specie per gli ambiti non prettamente tecnologici ma relativi invece alle problematiche della privacy e della protezione dei dati personali, assume un valore particolarmente importante per il "rispetto della garanzia delle vigenti disposizioni" da parte Sua.
17	x	predisporre e comunicare per iscritto al Titolare e al Responsabile privacy entro il 30 giugno 2009, e mantenere in seguito costantemente aggiornato, un elenco contenente gli estremi identificativi di eventuali altri amministratori di sistema che risultino soggetti alle Sue direttive, con indicazione delle funzioni rispettivamente ad essi assegnate in tale ambito autorizzato; La redazione e aggiornamento da parte Sua dell'elenco degli amministratoti di sistema, secondo le suddette modalità, è necessario per consentirci di adempiere l'obbligo normativo di rendere nota o conoscibile ai ns. dipendenti l'identità degli amministratori di sistema all'interno della ns. organizzazione attraverso apposita informativa ex art. 13 d.lgs. 196/2003 (in alternativa si possono utilizzare anche strumenti di comunicazione interna quali l'intranet aziendale, ordini di servizio a circolazione interna ecc.), nel caso in cui l'attività degli amministratori di sistema riguardi, anche indirettamente, servizi o sistemi che permettono il trattamento di dati personali di lavoratori.
18	x	ottenere e conservare a disposizione del responsabile privacy i curricula vitae dei suddetti amministratori di sistema, i cui contenuti dovranno essere conformi allo schema generale di curriculum previsto per Lei;
19	x	Nel caso di servizi di amministrazione di sistema affidati in outsourcing a terzi, Lei dovrà redigere e comunicare al Responsabile privacy gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.
		Misure di conformità operativa relative all'Amministratore di sistema
20	x	predisporre e mantenere aggiornati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte Sua (nella sua qualità di "amministratore di sistema"); tali registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste. Le registrazioni devono avere i riferimenti temporali certi e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo (non inferiore a sei mesi). Una soluzione possibile sono i processi di conservazione digitale in linea con le regole tecniche previste dall'art. 71 del Codice dell'amministrazione digitale, contenute nella deliberazione CNIPA n. 11/2004 e nel DPCM 13 gennaio 2004. La preghiamo di volerci comunicare per iscritto, improrogabilmente entro il termine del 30 giugno 2009, le procedure e modalità con le quali Lei ha implementato il suddetto sistema di registrazioni (access log) e come verrà garantita la verifica di tali registrazioni in conformità alle già menzionate Linee guida del Garante della privacy.

Nello svolgimento della propria attività, quale amministratore di sistema Lei è tenuto a rispettare sempre le seguenti regole:

		Operazioni sul/i server		
		ogni amministratore ha il proprio account e non usa mai quello generale (in modo da individuarne e registrarne l'attività);		
		l'Amministratore di sistema deve implementare un sistema di registrazione dei propri accessi ai sistemi informatici e ai database aziendali; deve essere garantita la completezza, inalterabilità e di tali registrazioni; deve essere assicurata la conservazione di tali registrazioni per un periodo di tempo di almeno 6 mesi;		
		Il/i server deve essere configurato in modo che siano attivi e raggiungibili solo i servizi effettivamente richiesti;		
		i servizi attivi devono essere configurati per rispondere alle sole esigenze richieste dall'ambiente in cui si trovano, facendo attenzione che eventuali malfunzionamenti non pregiudichino il funzionamento della macchina o di altri applicativi;		
		i guest account su qualsiasi sistema o hardware di rete (es. eventuali guest account abilitati di default sui sistemi operativi) devono essere disabilitati o eliminati, a parte eventuali server FTP (File Transfer PROTOCOL) con accesso anonimo abilitato approvato dalla Direzione o dal Responsabile privacy.		
		Misure di sicurezza specifiche per utenti privilegiati (root e Administrator):		
		utilizzare l'accesso ordinario per accedere ai propri file personali, limitando l'accesso privilegiato ad operazioni di amministrazione del sistema		
		utilizzare la propria autorità con moderazione e responsabilmente		

		limitare altri accessi privilegiati al proprio sistema e in generale ai sistemi, alle applicazioni e ai database; non bisogna creare account privilegiati o garantire privilegi di sistema a un account se non dietro autorizzazione dell'amministratore di sistema o, nel caso si tratti dello stesso amministratore di sistema, della Direzione della Società.		
		In presenza di applicazioni critiche (es. *web server, o altre applicazioni, come i gateway antivirus per la posta elettronica*) devono essere usati sistemi di filtro applicativo esterni o interni allo stesso server (cioè programmi che, partendo dalla conoscenza dell'applicazione da proteggere, agiscono come filtro che controlla la correttezza delle richieste all'applicazione: sanno quali sono corrette e bloccano quelle anomale). Occorre monitorare il sistema tenendo sotto osservazione in particolare i seguenti aspetti: ✓ tentativi di accesso falliti, ✓ accessi come utente privilegiato, ✓ file .RHOSTS, ✓ modifiche ai file di sistema, ✓ /VAR/ADM/MESSAGES o equivalenti ➢ activity log file (history o equivalenti) ➢ ecc.		
		Misure di sicurezza specifiche per password di default del fornitore		
		tutti i sistemi operativi e gli apparecchi collegati a server e PC, che all'inizio hanno una password di default del fornitore, devono cambiarla secondo la politica aziendale. Non cambiarla è un grave errore che mette a repentaglio l'azienda, perché le password id default sono notissime e facilmente reperibili sul web da parte di estranei.		
		Misure di sicurezza specifiche sulle password egli utenti non privilegiati L'Amministratore di sistema può **cambiare la password** di un account (anche non privilegiato) solo su richiesta del titolare dell'account. Chi riceve la richiesta di cambiamento della password deve richiamare il richiedente prima di intervenire, e la telefonata deve essere fatta non al numero fornito dal richiedente ma al numero che figura nell'elenco aziendale. Chi riceve la richiesta di cambiare la password deve inviare al richiedente una conferma mediante posta interna.		
		Tutte le richieste di **aumentare i privilegi** o i diritti di account devono essere approvate per iscritto dal superiore del titolare dell'account. Una v volta apportato il cambiamento, sarà necessario mandare una conferma al superiore del richiedente mediante posta interna. Inoltre, queste richieste devono essere verificate secondo le procedure di verifica e autorizzazione.		
		L'Amministratore di sistema può attivare un **nuovo account** per un soggetto autorizzato, solo su richiesta scritta firmata dal superiore del titolare del nuovo account oppure tramite e-mail munita di firma digitale (es. dell'Ufficio del Personale). Chi riceve la richiesta di attivare il nuovo account deve inviare al richiedente una conferma mediante posta interna.		
		L'Amministratore di sistema può **disattivare un account**, solo su richiesta scritta firmata dal superiore del titolare dell'account da disattivare oppure tramite e-mail munita di firma digitale di persona autorizzata (es. dell'Ufficio del Personale). Chi riceve la richiesta di disattivare un account deve inviare al richiedente una conferma mediante posta interna.		
		Misure di sicurezza specifiche per accessi da remoto		
		evitare di collegarsi come root dall'esterno della rete aziendale. L'accesso amministrativo via internet non è consentito.		
		non montare files di sistema (filesystem) da una connessione remota;		
		L'accesso remoto informatico alla rete aziendale deve essere fornito solo al personale che avrà dimostrato di averne giustificata necessità.		
		La richiesta deve essere presentata da un Amministratore di Sistema e l'identità e autorizzazione del richiedente, se non è persona nota all'Amministratore di Sistema, deve essere verificata secondo le modalità previste nella sezione "Procedure di verifica e autorizzazione" contenuta nel Documento Programmatico sulla Sicurezza.		
		L'accesso alla rete aziendale da remoto deve essere protetto tramite l'uso di sistemi di autenticazione forte come le smart card associate a password dinamiche (identificatori a tempo) o sistemi di riconoscimento tramite biometria, nonché mediante l'utilizzo di connessioni VPN o analoghe modalità sicure.		
		Misure di sicurezza specifiche per le password privilegiate		
		scegliere proprie password forti, composte da almeno 12 caratteri, alfanumerici, contenenti almeno un simbolo, almeno una lettera maiuscola e una minuscola, di contenuto comunque non reperibile da vocabolari in qualsiasi lingua o facilmente riconducibile all'interessato (es. veicolo, targa, indirizzo, telefono, compleanno, ecc.) o all'azienda,		
		evitare di utilizzare la stessa password per diversi account, o di utilizzare una variante di una password già usata, con un elemento che cambia e un altro che rimane lo stesso secondo uno schema prevedibile (es. kevin1, kevin2, KEVINGEN, KEVINFEB; oppure 743501, 743502, 743503 in cui gi ultimi due numeri corrispondono al mese in corso)		
		cambiare regolarmente le proprie password (almeno ogni 60 giorni);		
		non utilizzare la propria password da connessioni remote non sicure;		
		tutti gli account di amministratore di sistema devono scadere in automatico dopo un anno, al fine di evitare la sopravvivenza di account non più utilizzati, che potrebbero essere utilizzati da eventuali hacker per attacchi aziendali;		
		la password di utente privilegiato deve essere nota al Servizio IT o al referente esterno per gli interventi di amministrazione remota sui sistemi (v. sopra);		

		eventuali richieste di sistemare una password di account privilegiato devono essere approvate dall'Amministratore di sistema responsabile del PC relativo all'account; la nuova password deve essere inviata tramite posta interna (in tal caso le password devono essere contenute in buste sigillate così da oscurarne il contenuto) o consegnata di persona.		
		Le credenziali di autenticazione dell'amministratore di sistema o comunque affidate a quest'ultimo di regola non devono mai essere rivelate, senza la previa autorizzazione scritta della Direzione o di un eventuale capositore responsabile.		
		Le password statiche in chiaro non saranno registrate in alcun file né conservate come testo richiamabile premendo un tasto funzione.		
		Le credenziali di autenticazione dell'amministratore di sistema devono essere conservate in un file o database criptato, protetto da password, conservato in luogo fisico (es. cassaforte) o esterno sicuro (archivio web-BASED o similare) ovvero conservato con le specifiche modalità previste dal Documento Programmatico sulla sicurezza aziendale.		
		Altre misure di sicurezza specifiche: miscellanea		
		al momento del login verificare la provenienza dell'ultima sessione di lavoro;		
		evitare di utilizzare file o directory WORLD-WRITABLE;		
		è vietato installare programmi di monitoraggio pacchetti (network SNOOPING), se non ai limitati fini dell'effettuazione di test antintrusione, il cui esito va in ogni caso registrato secondo procedure da prevedersi allo scopo;		
		è vietato installare programmi di intercettazione password (sniffing, KEY-LOGGER), se non ai limitati fini dell'effettuazione di test antiintrusione, il cui esito va in ogni caso registrato secondo le procedure previste dal DPS;		
		evitare di usare programmi come IRC, ICQ o Napster come utente privilegiato, essendo programmi potenzialmente pericolosi.		
		l'utente che amministra personalmente come root o Administrator una macchina si assume tutte le responsabilità che questo comporta; in caso di necessità l'A.S. ha il diritto, comunque, di richiedere l'accesso al sistema.		
		Misure di sicurezza specifiche per l'accesso dei visitatori alle connessioni di rete		
		Tutti i punti di accesso Ethernet o wireless a portata di chiunque (es. prese ethernet o punti di accesso wireless installati/e nelle sale riunioni, in mensa, nei centri per la formazione o altre aree accessibili ai visitatori), devono essere su una rete segmentata per impedire accessi non autorizzati alla rete interna. L'amministratore di sistema può decidere di allestire una LAN virtuale in un commutatore, qualora possibile, per controllare l'accesso a questi punti.		
		Misure di sicurezza specifiche per richieste di esecuzione comandi o di apertura programmi		
		L'Amministratore di sistema non deve eseguire comandi o aprire programmi su richiesta di persona non nota. Nei casi in cui una persona non verificata sembra avere un valido motivo per avanzare tale richiesta, quest'ultima non andrebbe soddisfatta senza la pregressa identificazione personale del richiedente in conformità alla procedura prevista		
		Misure di sicurezza specifiche sulle richieste di assistenza L'Amministratore di sistema avendo account privilegiati non deve fornire assistenza o collaborazione ad alcuna persona non verificata. Questa policy si riferisce in particolare all'assistenza sull'hardware (come l'insegnamento all'uso delle applicazioni)) all'acceso ai database aziendali, allo scaricamento di software o alla rivelazione dei nomi dei colleghi con diritto di accesso remoto.		
		Misure di sicurezza specifiche sulle richieste e rivelazioni di informazioni		
		L'Amministratore di sistema non deve mai diffondere informazioni relative ai sistemi informatici dell'azienda o agli apparecchi correlati (es. procedure di acceso, punti esterni di accesso remoto, numeri di connessione, ecc.), senza avere prima identificato il richiedente. Ogni richiesta di informazioni deve essere vagliata in base alla politica aziendale di classificazione dei dati per decidere se il richiedente è autorizzato a detenere queste informazioni. Quando non è possibile decidere la classe delle informazioni, esse devono essere considerate ad uso interno. In certi casi i terzi fornitori dovranno essere in grado di comunicare con l'Amministratore di sistema per scopi di assistenza tecnica. In tali casi i fornitori dovranno essere invitati a rivolgersi a precisi contatti con il settore IT in modo da potersi conoscere di persona per una adeguata verifica.		
		Misure di sicurezza specifiche per le registrazioni di dominio		
		Quando ci si registra per ottenere un indirizzo internet o per un nome dell'HOST, le informazioni riguardanti il personale amministrativo, tecnico o altro non devono identificare alcuna persona per nome o tramite il numero di telefono. Deve invece essere presentato un indirizzo generico di e-mail (in forma tipo amministratore@azienda.com) e il numero telefonico principale dell'azienda.		
		Misure di sicurezza specifiche sulla formazione del personale		
		Il personale che accede in via privilegiata a sistemi, applicazioni, hardware e/o database, deve frequentare e completare con successo un corso di formazione sui temi della sicurezza prima che gli sia consentito accedere ai sistemi informativi aziendali.		

Le ricordiamo, che il provvedimento del Garante citato in premessa, obbliga il Titolare alla *"verifica*" almeno annuale delle attività dell'Amministratore di Sistema, onde controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

Pertanto, l'**AZIENDA DI PROMOZIONE E SVILUPPO TURISTICO DI LIVIGNO S.R.L.** si riserva riserva di effettuare, in qualsiasi momento e con le modalità discrezionalmente ritenute più opportune, gli controlli circa la conformità della sua attività alle direttive impartite.

Sulla base di quanto previsto al punto sopra citato, la informiamo che i suoi estremi identificativi saranno riportati nel MOP dell'**AZIENDA DI PROMOZIONE E SVILUPPO TURISTICO DI LIVIGNO S.R.L.,** oppure annotati comunque in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.

La presente procedura verrà fatta sottoscrivere per accettazione anche ai consulenti IT che la Società incarica dei suddetti compiti.

Per quanto non previsto e non riportato sul presente atto di nomina si rinvia alla normativa vigente in materia di protezione e sicurezza dei dati personali.

Presa visione del presente atto di nomina e nel rispetto della normativa vigente, dichiara di accettare l'incarico di Amministratore di Sistema.

Livigno lì _____

Titolare del trattamento

Sig. **LUCA MORETTI**

per accettazione

_____