Alfa
Agenzia regionale per il lavoro
la formazione e l'accreditamento

**Allegato sub 5**

**Requisiti tecnici indispensabili del PC (personale del dipendente) da cui si effettua la connessione alla LAN di ALFA:**

1. sistema operativo Windows 8 o 10 (esclusi Windows XP, Vista, ME e 7) [consentito anche MAC OS]
2. applicativo antivirus installato, licenziato e costantemente aggiornato
3. autorizzare il Servizio Sistemi Informativi all'accesso da remoto al PC per verificare la rispondenza ai requisiti di cui ai punti 1. e 2., nonché alla verifica di compatibilità dei programmi installati e all'eventuale installazione di nuovi in relazione alle attività lavorative assegnate
4. in seguito della verifica di cui a tutti i punti precedenti, potrà essere espresso parere positivo alla possibilità di collegamento sulla LAN di ALFA

**Modalità comportamentali del personale coinvolto**

1. Ogni utente è responsabile, civilmente e penalmente, del corretto uso delle risorse informatiche, con particolare riferimento ai servizi, ai programmi cui ha accesso e ai dati trattati a fini istituzionali
2. Per l'utilizzo dei sistemi informatici dell'Ente il dipendente accede mediante VPN SSL (Virtual Private Network), il cui client software deve essere installato sul proprio PC, con le credenziali fornite
3. Le credenziali per l'accesso sono costituite da un codice identificativo personale (username o user id) e da una parola chiave (password) che deve essere strettamente personale, segreta. Ogni utente è responsabile civilmente e penalmente della custodia e della segretezza delle proprie credenziali (D.lgs 196/2003 e s.m.i.), le quali sono incedibili. Le credenziali non devono mai essere salvate sul PC in uso e sui browser di accesso agli applicativi
4. Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico dell'Amministrazione mediante virus, malware o mediante ogni altro software aggressivo, quali l'apertura di messaggi di posta elettronica e dei relativi allegati di provenienza sospetta o non conosciuta e affidabile
5. Ogni utente deve verificare la presenza e il regolare funzionamento del software antivirus e antimalware installato sul proprio computer
6. L'utente è tenuto ad utilizzare le unità di rete per la condivisione di informazioni strettamente professionali; non può pertanto collocare, anche temporaneamente, in queste aree qualsiasi file che non sia attinente allo svolgimento dell'attività lavorativa. L'utente è tenuto, altresì, alla periodica revisione dei dati presenti in tutti gli spazi assegnati, con cancellazione dei files che non necessitano di archiviazione e che non siano più necessari ai fini procedimentali. Particolare attenzione deve essere prestata alla duplicazione dei dati al fine di evitare, salvo casi eccezionali, un'archiviazione superflua
7. I profili di navigazione internet sono applicati a seconda dell'attività professionale svolta. Attraverso tale profilazione, saranno consentite le attività di accesso, navigazione, registrazione a siti web, scaricamento (download), ascolto e visione di file audio/video in modo personalizzato e correlato con la propria attività lavorativa, e comunque sempre in maniera dipendente delle risorse di banda disponibili al momento nella rete. Ogni variazione all'applicazione del profilo di navigazione

standard (di base), deve essere formalizzata dal Dirigente responsabile di Settore, il quale motiva la richiesta indicando eventualmente se questa debba essere limitata nel tempo

8. Sono applicate politiche per la sicurezza della rete di trasmissione dati attraverso sistemi di "filtraggio" dei contenuti e pagine web, i quali bloccano o quantomeno limitano la navigazione su categorie di siti ben specifiche che siano potenzialmente illegali secondo normativa vigente (quali pedofilia, gioco d'azzardo, ecc.) o comunque ledenti la dignità umana (violenza, razzismo, …). Non è consentito scambiare materiale protetto dalla normativa vigente in tema di tutela del diritto d'autore e utilizzare sistemi di scambio dati/informazioni con tecnologie "peer to peer" (dall'interno della rete all'esterno e viceversa) o sistemi di anonymous proxy
9. La casella di posta elettronica assegnata da ALFA al dipendente è uno strumento di lavoro. Gli assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. La casella di posta, da casa, deve essere esclusivamente utilizzata tramite accesso web
10. In ogni caso non è consentito utilizzare tecniche di "mail spamming" (invio massiccio di comunicazioni), utilizzare il servizio di posta elettronica per inoltrare contenuti non attinenti alle materie di lavoro; trasmettere con dolo, virus, worms, Trojan o altro codice maligno, finalizzati ad arrecare danni e malfunzionamenti ai sistemi informatici
11. È altamente raccomandato di attenersi alle nome precedenti (punti 4,.5., 9., 10.) anche al di fuori della connessione in VPN alle risorse dell'Ente
12. In ogni caso si rimanda alle disposizioni già in essere e pubblicate sulla Intranet di ALFA:
    a. MINACCE ALLA SICUREZZA INFORMATICA - Regole di comportamento (http://10.22.1.175:8000/docs/SistemiInformativi/regole_di_comportamento_v2.pdf)
    b. Buone regole per nominare i file e le cartelle (http://10.22.1.175:8000/docs/SistemiInformativi/nomi_file_e_lunghezza_percorsi.pdf)
    c. Le istruzioni e i manuali necessari sono pubblicati sulla Intranet di ALFA (http://10.22.1.175:8000/index.php/servizi/16-sistemi-informativi)

ALFA si riserva di effettuare verifiche sul corretto utilizzo della posta elettronica, di Internet, nel rispetto delle normative vigenti e del presente documento

Le disposizioni generali contenute nel presente documento possono essere soggette ad aggiornamenti, integrazioni e/o correzioni, in relazione all'evolversi della tecnologia, all'entrata in vigore di sopravvenute disposizioni di legge o all'evolversi delle esigenze di ALFA.