All.to 1

**LAVORO AGILE**

**ALLEGATO TECNICO**

**SPECIFICHE TECNICHE MINIME DI SICUREZZA DEI DISPOSITIVI ELETTRONICI E DEI SOFTWARE, NONCHÉ REGOLE NECESSARIE A GARANTIRE LA PROTEZIONE DEI DATI E DELLE INFORMAZIONI**

*Sommario*

Art. 1 Oggetto - Ambito di applicazione

Art. 2 Principi generali

Art. 3 Dotazioni informatiche ai dipendenti nell’ambito della modalità di lavoro agile

Art. 4 Modalità di accesso ai servizi informatici dell’Amministrazione.

Art. 5 Modalità di utilizzo degli strumenti informatici

Art. 6 Gestione delle password e degli account

Art. 7 Protezione antivirus e antimalware

Art. 8 Utilizzo delle periferiche e delle cartelle condivise

Art. 9 Dispositivi di archiviazione e salvaguardia dei dati

Art. 10 Gestione e utilizzo della posta elettronica

Art. 11 Controlli, responsabilità e sanzioni

Art. 12 Aggiornamenti delle regole tecniche

**Art. 1 Oggetto - Ambito di applicazione**

**1.** Il presente documento individua le specifiche tecniche minime di sicurezza dei dispositivi elettronici e dei *software*, nonché le regole necessarie a garantire la protezione dei dati e delle informazioni dell’Amministrazione. In particolare, disciplina le modalità di accesso e utilizzo degli strumenti informatici, di internet, della posta elettronica.

**2.** Gli strumenti informatici sono costituiti dall'insieme delle risorse informatiche dell’Amministrazione, ovvero dalle risorse infrastrutturali e dal patrimonio informativo digitale (dati).

**3.** Le risorse infrastrutturali sono costituite dalle componenti *hardware* e *software*.

**4.** Il patrimonio informativo è l'insieme delle banche dati in formato digitale e in generale di tutti i documenti prodotti tramite l'utilizzo delle risorse infrastrutturali.

**5.** Le prescrizioni del presente documento si applicano ai dipendenti dell’Amministrazione coinvolti nell’attività del lavoro agile, in attuazione di quanto previsto dall’articolo 14 della legge 7 agosto 2015, n. 124 e dalla direttiva del Presidente del Consiglio dei Ministri del 1° giugno 2017, n. 3.

**Art. 2 Principi generali**

**1.** L’Amministrazione promuove l'utilizzo degli strumenti informatici, di Internet, della posta elettronica e della firma digitale quali mezzi utili a perseguire con efficacia ed efficienza le proprie finalità istituzionali, e specificatamente l’obiettivo di introduzione del “lavoro agile” o “smart working”, quale modalità flessibile di esecuzione del rapporto di lavoro subordinato finalizzata a incrementare la produttività e agevolare la conciliazione dei tempi di vita e di lavoro in accordo con le linee guida e i principi delineati dalla normativa vigente.

**2.** L'Amministrazione promuove ogni opportuna misura organizzativa e tecnologica, volta a prevenire il rischio di utilizzi impropri delle strumentazioni messe a disposizione dall’Amministrazione anche nell’ambito dello svolgimento dell’attività di lavoro agile.

**3.** 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. È altresì responsabile del contenuto delle comunicazioni effettuate e ricevute a fini istituzionali anche per quanto attiene la riservatezza dei dati ivi contenuti, la cui diffusione impropria potrebbe configurare violazione del segreto d'ufficio o della normativa per la tutela dei dati personali. Sono vietati comportamenti che possono creare un danno, anche di immagine, all'Amministrazione.

**4.** Ogni utente coinvolto nell’attività del lavoro agile, indipendentemente dalla posizione che ricopre all’interno della struttura organizzativa dell’Amministrazione è vincolato ad applicare le norme descritte nel presente documento.

**5.** Il lavoratore deve custodire le credenziali, la posta elettronica e gli altri servizi informatici e telematici in modo appropriato e diligente ed è responsabile della propria postazione di lavoro.

**6.** L’Ufficio CED supporta il servizio di assistenza agli utenti (in seguito anche lavoratori agili), avvalendosi di personale specializzato, sia esso personale dipendente dell’Amministrazione stessa, sia personale esterno.

**Art. 3 Modalità di accesso dei dipendenti nell’ambito del lavoro agile**

**1.** Al dipendente in modalità di lavoro agile sono attribuite le credenziali di autenticazione per l’accesso ai servizi informatici dell’Amministrazione. Di regola le credenziali in questione sono quelle già possedute dal dipendente per ragioni d’ufficio.

**Art. 4 Modalità di accesso ai servizi informatici dell’Amministrazione**

**1.** Il dipendente in modalità di lavoro agile accede ai servizi informatici resi disponibili dall’Amministrazione.

**2.** Per l’uso dei servizi di cui al comma 1 il dipendente accede mediante VPN (*Virtual Private Network*) in caso di utilizzo di piattaforme caricate su server provinciali in alternativa il worker utilizza piattaforme in Cloud.

**3.** In caso di utilizzo dell’infrastruttura Server Provinciale il dipendente si collegherà ai servizi applicativi mediante VPN opportunamente configurata, il cui accesso sarà garantito tramite le credenziali di cui al comma 2 dell’articolo 3, utilizzerà una propria postazione di lavoro virtuale, dotata di strumenti di *office automation*, protezione dei dati, di posta elettronica, accesso ad Internet con i relativi servizi di *collaboration*.

**4.** Il dipendente agile dispone dei servizi applicativi utili allo svolgimento dell’attività lavorativa in coerenza con l’accordo individuale di lavoro stipulato con l’Amministrazione.

**Art. 5 Modalità di utilizzo degli strumenti informatici**

**1.** AI fine di evitare di introdurre virus o pericoli similari nella rete, è raccomandato di non copiare file di provenienza incerta da supporti quali *pen-drive*, memorie esterne per finalità non attinenti alla propria prestazione lavorativa.

**2.** Non è consentita la consultazione, memorizzazione e diffusione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;

**3.** È consentita esclusivamente l'installazione di supporti per la connessione mobile per l'accesso a Internet messi a disposizione dall’Amministrazione o da essa autorizzati. Qualunque esigenza in tal senso deve essere comunicata all’Ufficio CED, che ha il compito di analizzare la problematica per addivenire a una soluzione coerente con le vigenti politiche di sicurezza e integrità della rete.

**Art. 6 Gestione delle password e degli account**

**1.** Le credenziali per l’accesso alle postazioni di lavoro oppure ai servizi informatici sono costituite da un codice identificativo personale (username o user id) e da una parola chiave (password) e in alcuni casi da un codice PIN.

**2.** Laddove non diversamente previsto, la password deve essere composta da almeno otto caratteri e formata da lettere (sia maiuscole che minuscole) e numeri e/o caratteri speciali.

**3.** La password non deve contenere riferimenti agevolmente riconducibili all'utente e comunque va cambiata regolarmente per motivi di sicurezza.

**4.** La password e/o il PIN di qualunque strumento/servizio deve essere strettamente personale, segreta. Ogni individuo è responsabile civilmente e penalmente della custodia e della segretezza delle proprie credenziali, le quali sono incedibili.

**5.** È consentito l’accesso alla postazione di lavoro o a un servizio informatico esclusivamente utilizzando le proprie credenziali di autenticazione.

**6.** È compito dell’Ufficio personale comunicare all’Ufficio CED competente in materia di sistemi informativi eventuali variazioni del personale in lavoro agile al fine di aggiornare, creare, modificare e cancellare gli account, nonché eventuali autorizzazioni sui sistemi.

**Art. 7 Protezione antivirus e antimalware**

**1.** nel caso il collegamento avvenga mediante VPN, l’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; la navigazione su siti web per ragioni non riconducibili all’attività lavorativa e così via.

**2.** In ogni caso l’utente è tenuto a controllare la presenza e il regolare funzionamento del software antivirus e antimalware eventualmente installato sul proprio computer portatile.

**3.** Il dipendente agile deve eseguire scansionipianificate, allo scopo di verificare l’eventuale presenza di codice malevolo, da porre in quarantena.

**Art. 8 Utilizzo delle periferiche e delle cartelle condivise**

**1.** Per periferica condivisa si intende stampante, scanner o qualsiasi altro dispositivo elettronico che può essere utilizzato in contemporanea da più uffici. Per cartella condivisa (o “area di lavoro condivisa” o “condivisione”) si intende uno spazio disco disponibile sui server centrali, per la memorizzazione di dati e programmi accessibili ad un gruppo di utenti preventivamente autorizzati, oppure anche ad un solo utente nel caso di utilizzo a scopo di backup o comunque spazio disco su una piattaforma in cloud.

**2.** Gli utenti autorizzati possono accedere ad una determinata area di lavoro condivisa nella quale si indica, il nome dell’area condivisa da creare/modificare e gli utenti interessati alla scrittura dei dati oppure alla sola lettura degli stessi.

**3.** 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 file 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.

**4.** L'utilizzo delle periferiche condivise è riservato esclusivamente ai compiti di natura strettamente istituzionale, come tutti gli spazi di archiviazione messi a disposizione degli utenti da parte dell’Amministrazione.

**Art. 9 Dispositivi di archiviazione e salvaguardia dei dati**

**1.** Fatte salve le politiche di salvataggio centralizzato dei dati conservati sui sistemi informatici e sulle postazioni di lavoro virtuali dei lavoratori agili, è consentito l’eventuale uso di dispositivi di backup via USB (chiavette, hard disk esterni, ecc.) purché i dati in essi contenuti siano comunque trattati ai sensi della normativa vigente in materia di dati personali, sensibili o giudiziari, e non vengano in nessun modo ceduti a terzi, se non nel perimetro della normativa citata e del trattamento necessario ai fini procedimentali.

**2.** Ogni utente è responsabile della custodia dei dati di lavoro presenti sulla propria postazione di lavoro informatica. Gli utenti hanno cura di conservare copia della documentazione di lavoro nelle aree condivise predisposte.

**Art. 10 Gestione e utilizzo della posta elettronica**

**1.** La casella di posta elettronica assegnate dall’Amministrazione al lavoratore agile è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

**2.** 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.

**Art. 11 Controlli, responsabilità e sanzioni**

**1.** L'Amministrazione si riserva di effettuare verifiche sul corretto utilizzo degli strumenti informatici, della posta elettronica e delle dotazioni informatiche, nel rispetto delle normative vigenti e del presente documento.

**2.** La violazione da parte degli utenti dei principi e delle norme contenute nel presente documento comporta l'applicazione delle sanzioni previste dalle disposizioni contrattuali vigenti in materia, previo espletamento del procedimento disciplinare.

**Art. 12 Aggiornamenti delle regole tecniche**

**1.** 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 dell’Amministrazione.

Data………………….. Firma del dipendente per accettazione

…………………………………………..