Specifiche tecniche minime di custodia e sicurezza dei dispositivi elettronici e dei software, nonché regole necessarie a garantire la protezione dei dati e delle informazioni

- Allegato A all'Accordo Individuale di Lavoro Agile –

Allegato A – Specifiche tecniche informatica

Art. 1 Oggetto - Ambito di applicazione

1. Il presente documento individua le specifiche tecniche minime di custodia e sicurezza dei dispositivi elettronici e dei software, nonché le regole necessarie a garantire la protezione dei dati e delle informazioni della Regione Abruzzo (di seguito anche Amministrazione). In particolare, disciplina le modalità di accesso ed utilizzo degli strumenti informatici, di internet, della posta elettronica, eventualmente messi a disposizione dall'Ente ai suoi utenti, intesi come dipendenti nell'ambito della modalità di lavoro agile (in seguito anche *smart working*) a cui sia stato concesso l'uso di risorse informatiche di proprietà dell'Amministrazione ovvero che utilizzino risorse infrastrutturali proprie.

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 ed 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 regionale coinvolti nell'espletamento dell'attività lavorativa in modalità agile.

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 ad 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 e delle banche dati di proprietà dell'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 alla 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 nel 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. Gli strumenti informatici eventualmente messi a disposizione del lavoratore agile (ad esempio, computer portatile, accessori, *software*, ecc.) sono di proprietà dell'Amministrazione. Il lavoratore

deve custodire ed utilizzare gli strumenti informatici, Internet, la posta elettronica e i servizi informatici e telematici in

modo appropriato e diligente, rimanendo responsabile della propria postazione anche se di sua proprietà.

6. Il Servizio Informatica e Statistica, competente in materia di sistemi informativi (in seguito anche "Sistemi Informativi"), supporta il servizio di assistenza agli utenti (in seguito anche lavoratori agili), avvalendosi di personale specializzato, sia esso personale dipendente dell'Amministrazione stessa, che personale esterno *in outsourcing*.

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

1. Al dipendente in modalità di lavoro agile sono resi disponibili una serie di strumenti software che costituiscono una postazione di lavoro virtuale.

2. 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 eventualmente con l'aggiunta del doppio fattore di autenticazione.

3. Per l'accesso agli strumenti di cui al comma 1, è consentito l'utilizzo di dispositivi (PC o Tablet) e connettività di tipo personali rispettando i requisiti di sicurezza di cui all'art. 6 comma 2

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 tramite i software messi a disposizione dall'Ufficio competente in Informatica dell'Usr.

2. Per l'utilizzo dei servizi di cui al comma 1 il dipendente accede agli strumenti mediante sistema di autenticazione, seguendo scrupolosamente le indicazioni riportate nella stessa sezione del portale.

3. L'Amministrazione rende disponibile gli strumenti *software* necessari per l'utilizzo dei servizi applicativi di cui al successivo comma 4 in un contesto di sicurezza.

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.

5. Gli strumenti *software* di cui al comma 3 sono utilizzabili anche durante l'espletamento dell'attività lavorativa presso l'ordinaria sede di servizio.

Art. 5 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) ed in alcuni casi da un codice PIN.

2. 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 (D.lgs. 196/2003 e s.m.i.), le quali sono incedibili.

3. È consentito l'accesso alla postazione di lavoro o ad un servizio informatico esclusivamente utilizzando le proprie credenziali di autenticazione.

4. È compito di ogni singolo Dirigente comunicare tempestivamente al Servizio Informatica e Statistica, mediante l'apposita procedura informatica, eventuali

variazioni del personale in lavoro agile al fine di aggiornare, creare, modificare e cancellare gli account, nonché eventuali autorizzazioni sui sistemi.

Art. 6 Protezione antivirus e *antimalware*

1. 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.

2. Ad ogni utente si raccomanda di verificare la presenza e il regolare funzionamento del software antivirus e *antimalware* installato sul proprio computer. In caso di utilizzo di dispositivi personali, è possibile utilizzare anche antivirus di tipo "*free*".

Art. 7 Ulteriori indicazioni comportamentali per gli utenti in lavoro agile

1. In caso ci si allontani dal pc, bloccare il pc in modo che non sia utilizzabile da altri (attivare il blocco schermo).

2. Non consentire a personale non esplicitamente autorizzato di visualizzare le informazioni a cui si ha accesso.

3. Non lasciare incustodite le credenziali con password per accedere agli applicativi utilizzati a fini di lavoro.

4. Non effettuare foto, "*print screen*" o cattura dello schermo nel corso di una sessione di lavoro o quando si ha accesso ad informazioni e/o dati per motivi di lavoro.

Art. 8 Utilizzo delle periferiche e delle cartelle condivise

1. Per cartella condivisa (o "area di lavoro condivisa" o "condivisione" o file sharing) 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 come area temporanea di lavoro.

2. Gli utenti autorizzati, per il tramite del servizio di "file sharing", 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 gli spazi 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 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 di tutti gli spazi di archiviazione messi a disposizione degli utenti da parte dell'Amministrazione è riservato esclusivamente ai compiti di natura strettamente istituzionale.

Art. 9 Produzione documentale, dispositivi di archiviazione e salvaguardia dei dati

1. La produzione documentale avviene esclusivamente utilizzando gli strumenti di produttività individuale messi a disposizione dall'Amministrazione e presenti in Radrive o in altri servizi web. È fatto divieto di produrre documenti con software personali o comunque non preventivamente autorizzati dalla struttura informatica regionale.

2. Ogni utente è responsabile della custodia dei dati/file di lavoro presenti sulla propria postazione di lavoro informatica. Gli utenti hanno cura di conservare la documentazione nel sistema documentale (Archiflow) o nelle aree di lavoro condivise predisposte dai Sistemi Informativi.

3. È fatto divieto di salvare e/o conservare documenti su dispositivi personali (PC, tablet, hard disk esterni, chiavette USB,…) e/o *cloud* esterni, salvo previa esplicita autorizzazione dei Sistemi Informativi regionali.

4. È fatto divieto di condividere o trasmettere documenti e dati con strumenti diversi da quelli messi a disposizione dall'Amministrazione (Radrive, Archiflow). E' altresì possibile utilizzare la posta elettronica per lo scambio di file seguendo le disposizioni specifiche di cui al comma 2 art. 13.

Art. 10 Utilizzo di Internet

1. Nell'ambito della propria infrastruttura informatica, l'Amministrazione si riserva di applicare diversi profili di navigazione, 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.

2. Ogni variazione all'applicazione del profilo di navigazione standard (di base), deve essere formalizzata dal Dirigente responsabile, il quale motiva la richiesta indicando eventualmente se questa debba essere limitata nel tempo.

3. 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*.

4. I dati di navigazione degli utenti sono raccolti mediante *log* a norma di legge e possono essere utilizzati, ma non diffusi, dai Sistemi Informativi per il monitoraggio delle funzionalità tecniche, per la risoluzione di problematiche, per scopi di sicurezza e per la raccolta di dati statistici aggregati ed anonimi, aventi il fine di migliorare la qualità e la fruibilità delle informazioni e dei servizi informatici e telematici.

5. I *log* sono conservati per 365 giorni per consentirne la consultazione alle autorità competenti in caso di abusi e poi automaticamente cancellati. In ogni caso

l'accesso a tali dati è consentito esclusivamente previa richiesta formale delle autorità competenti nei casi e con le procedure previsti dalla legge vigente.

Art. 11 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; va inoltre prestata attenzione a non trasmettere virus, *worms*, *Trojan* o altro codice maligno, avendo consapevolezza che possono arrecarsi danni e malfunzionamenti ai sistemi informatici dell'Amministrazione.

3. Il dipendente in lavoro agile accede al servizio di posta elettronica tramite webmail.

4. Al dipendente in lavoro agile è consentito l'utilizzo del servizio di posta elettronica per lo scambio dei documenti seguendo le disposizioni specifiche di cui al comma 2, art. 13.

Art. 12 Controlli, responsabilità e sanzioni

1. L'Amministrazione si riserva di effettuare verifiche sul corretto utilizzo degli strumenti informatici.

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.

Art. 13 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.