MINISTERO DELL'INTERNO

Ministero dell'Interno

DIPARTIMENTO PER LE POLITICHE DEL PERSONALE DELL'AMMINISTRAZIONE CIVILE E PER LE RISORSE STRUMENTALI E FINANZIARIE

BOZZA

LAVORO AGILE

(SMART WORKING)

REGOLAMENTO PER LA FASE SPERIMENTALE

ALLEGATO

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

Sommario

BOZZA

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 del Dipartimento per le politiche del personale dell'amministrazione civile e per le risorse strumentali e finanziarie (in seguito anche Amministrazione). In particolare, disciplina le modalità di accesso ed utilizzo degli strumenti informatici, di internet, della posta elettronica, eventualmente messi a disposizione del Dipartimento per le politiche del personale dell'amministrazione civile e per le risorse strumentali e finanziarie 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 in caso di utilizzo di risorse informatiche di proprietà del lavoratore agile*~~.
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 civile dell'Interno coinvolti nell'avvio del progetto pilota per la sperimentazione 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 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 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'avvio del progetto pilota per la sperimentazione del lavoro agile, indipendentemente dalla posizione che ricopre all'interno della macrostruttura organizzativa dell'Amministrazione è vincolato ad applicare le norme descritte nel presente documento.
5. Gli strumenti informatici 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 gli servizi informatici e telematici in modo appropriato e diligente ed è responsabile della propria postazione di lavoro.
6. La struttura dipartimentale competente in materia di sistemi informativi (in seguito anche "Sistemi Informativi") supporta il servizio di assistenza agli utenti (in seguito anche lavoratori agili),

BOZZA

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 è assegnata la dotazione informatica minima di cui ai punti successivi:
   a) personal computer portatile completo di sistema operativo e software per l'accesso alla rete interna dell'Amministrazione;
   b) SIM con relativo supporto hardware per la connessione ad Internet.

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.

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'utilizzo dei servizi di cui al comma 1 il dipendente accede mediante VPN SSL (Virtual Private Network) e un sistema di autenticazione forte a doppio fattore.
3. Il dipendente agile, dopo il collegamento alla VPN dell'Amministrazione e tramite le credenziali di cui al comma 2 dell'articolo 3, utilizza 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. L'Amministrazione rende disponibile sulla postazione di lavoro virtuale gli strumenti *software* necessari per l'utilizzo dei servizi applicativi di cui al successivo comma 5 in un contesto di sicurezza e omogeneizzazione delle stesse postazioni di lavoro.
5. 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.
6. La postazione di lavoro virtuale di cui al comma 3 è utilizzata anche durante l'espletamento dell'attività lavorativa presso l'ordinaria sede di servizio.

Art. 5 Modalità di utilizzo degli strumenti informatici

1. Il computer portatile o eventualmente altro *device* mobile affidato al lavoratore agile è uno strumento di lavoro. Ogni utilizzo improprio, non inerente all'attività lavorativa può contribuire a creare disservizi anche agli altri utenti, nonché minacce alla sicurezza informatica.
2. Per evitare il grave pericolo di introdurre *virus* e *malware* informatici nei sistemi dell'Amministrazione, devono essere utilizzati esclusivamente programmi messi a disposizione e distribuiti dall'Amministrazione stessa; in particolare è vietato scaricare file e software, anche gratuiti, prelevati da Internet, se non attinenti alle mansioni d'ufficio, ed in questo caso comunque su espressa autorizzazione della struttura dipartimentale competente in materia di sistemi informativi che provvederà materialmente all'installazione.
3. Non è consentito disinstallare o inabilitare il programma antivirus e antimalware installato dai Sistemi Informativi; ogni eventuale malfunzionamento di quest'ultimo, va segnalato tempestivamente alla predetta struttura dipartimentale competente in materia di sistemi informativi.
4. Non è consentito modificare la configurazione impostata sul proprio computer portatile o eventualmente altro *device* mobile, nonché installare periferiche (hard-disk, DVD, fotocamere, apparati multimediali, ecc ...) esterne agli strumenti in dotazione se non per esigenze di servizio, autorizzate dai Sistemi Informativi che provvederanno materialmente all'installazione.

BOZZA

5. Al fine di evitare di introdurre virus o pericoli similari nella rete, è raccomandato di non copiare file di provenienza incerta da supporti quali *pendrive*, memorie esterne per finalità non attinenti alla propria prestazione lavorativa.
6. 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;
7. 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 ai Sistemi Informativi, che hanno il compito di analizzare la problematica per addivenire ad una soluzione coerente con le vigenti politiche di sicurezza ed integrità della rete.
8. L'eventuale malfunzionamento o danneggiamento degli strumenti informatici deve essere tempestivamente comunicato ai Sistemi Informativi.
9. Il personale sistemistico e tecnico-informatico dei Sistemi informativi, incaricato della gestione e della manutenzione dei componenti del sistema informatico dipartimentale, possono accedere alle postazioni di lavoro anche con strumenti di supporto/assistenza e diagnostica remota, per effettuare interventi di manutenzione preventiva e correttiva, richiesti dall'utente, oppure in caso di oggettiva necessità, a seguito di rilevazione di problemi tecnici sulla postazione. Gli operatori di norma non accedono ai dati di lavoro, a meno che l'intervento richiesto non sia focalizzato su questi ultimi, e comunque esclusivamente alle componenti hardware/software strettamente necessarie alla risoluzione della problematica e sono tenuti rigorosamente al rispetto del segreto d'ufficio e delle norme vigenti sulla privacy.
10. Ogni dipendente che, per qualsiasi motivo, lasci incustodita la propria postazione di lavoro è tenuto a bloccare l'accesso al computer portatile stesso o spegnere fisicamente l'apparato in questione.

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) ed in alcuni casi da un codice PIN.
2. Laddove non diversamente previsto, la password deve essere composta da almeno quattordici 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. Essa ha la durata massima di sei mesi, trascorsi i quali deve essere modificata dall'utente, anche se non richiesto dal sistema. Nel caso di trattamento dei dati sensibili o giudiziari, la password utilizzata dagli incaricati al trattamento ha una durata massima di tre mesi, trascorsi i quali deve essere sostituita.
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 (D.lgs 196/2003 e s.m.i.), le quali sono incedibili.
5. È consentito l'accesso alla postazione di lavoro o ad un servizio informatico esclusivamente utilizzando le proprie credenziali di autenticazione.
6. In caso di cessazione del rapporto di lavoro in modalità agile dovrà essere cura dell'utente rimuovere ogni dato personale eventualmente presente sulle macchine in dotazione, prima che l'account individuale del dipendente venga disattivato.
7. È compito della competente struttura dipartimentale per la gestione delle risorse umane comunicare alla struttura dipartimentale 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.

BOZZA

Art. 7 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; la navigazione su siti web per ragioni non riconducibili all'attività lavorativa e così via.
2. Ogni utente è tenuto a controllare la presenza e il regolare funzionamento del software antivirus e antimalware eventualmente installato sul proprio computer portatile.
3. Nel caso che il software antivirus e antimalware rilevi la presenza di un virus e/o di un malware che non è riuscito ad eliminare, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer portatile e segnalare tempestivamente l'accaduto alla struttura dipartimentale competente in materia di sistemi informativi.
4. Ogni dispositivo magnetico di provenienza esterna all'Amministrazione dovrà essere verificato mediante il programma antivirus e antimalware prima del suo utilizzo e, nel caso venga rilevato un virus e/o malware non eliminabile dal software, non dovrà essere utilizzato.
5. Sulle postazioni di lavoro in dotazione al dipendente agile l'Amministrazione esegue scansioni pianificate allo scopo di verificare l'eventuale presenza di codice maligno 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*.
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 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.
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 delle strutture Informatiche 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, etc.) 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 con il supporto dei Sistemi Informativi.

BOZZA

Art. 10 Utilizzo di Internet

1. La risorsa Internet è per sua natura limitata nella banda di navigazione disponibile. Ferme restando le modalità di utilizzo degli strumenti informatici di cui all'art. 3, l'utilizzo di Internet deve essere circoscritto agli scopi inerenti l'attività lavorativa. L'utente è direttamente responsabile dell'uso del servizio Internet, dei contenuti ricercati e visitati e delle informazioni che vi immette.
2. 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.
3. Ogni variazione all'applicazione del profilo di navigazione standard (di base), deve essere formalizzata dal Dirigente responsabile di Area, il quale motiva la richiesta indicando eventualmente se questa debba essere limitata nel tempo.
4. 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*.
5. La categorizzazione di cui al comma 4, è effettuata anche con l'ausilio di strumenti automatici e pertanto può contenere errori o inesattezze, e può essere integrata o corretta, mediante segnalazione, alla struttura dipartimentale competente in materia di sistemi informativi.
6. I dati di navigazione degli utenti, sono raccolti mediante *log* a norma di legge e possono essere utilizzati ma non diffusi dalla struttura dipartimentale competente in materia di sistemi informativi per il monitoraggio delle funzionalità tecniche, per la risoluzione di problematiche, per scopo di sicurezza e per 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.
7. I *log* sono conservati per centottanta 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; trasmettere con dolo, virus, worms, Trojan o altro codice maligno, finalizzati ad arrecare danni e malfunzionamenti ai sistemi informatici.

Art. 12 Controlli, responsabilità e sanzioni

1. Il computer portatile o altro apparato in dotazione al dipendente agile è configurato dall'Amministrazione in modo da consentirne l'utilizzo esclusivamente per finalità lavorative e per la salvaguardia della sicurezza e dell'integrità dei dati e dell'infrastruttura tecnologica.
2. L'Amministrazione si riserva di effettuare verifiche sul corretto utilizzo degli strumenti informatici, della posta elettronica, di Internet, nel rispetto delle normative vigenti e del presente documento.

3. 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.
4. Delle violazioni al presente regolamento, compiute da utenti esterni all'organigramma dell'Ente.

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.

BOZZA