ALLEGATO A)

MANUALE OPERATIVO PER IL CORRETTO UTILIZZO DEI DISPOSITIVI INFORMATICI, POSTA ELETTRONICA E TRATTAMENTO DEGLI ARCHIVI INFORMATICI

Art. 1 – Oggetto e Ambito di applicazione

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 dell'Amministrazione. In particolare, disciplina le modalità di accesso e utilizzo degli strumenti informatici, di internet, della posta elettronica, eventualmente messi a disposizione dall'Amministrazione ai suoi utenti, intesi come dipendenti nell'ambito della modalità di lavoro a distanza 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.

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

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.

Art. 2 – Principi generali

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 a distanza (da remoto o agile), 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.

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 a distanza.

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.

Ogni utente coinvolto nell'avvio del lavoro a distanza, indipendentemente dalla posizione che ricopre all'interno della struttura organizzativa

dell'Amministrazione è vincolato ad applicare le norme descritte nel presente documento.

Gli strumenti informatici messi a disposizione del lavoratore (ad esempio, computer portatile, accessori, software, ecc.) sono di proprietà dell'Amministrazione. Il lavoratore deve custodire e utilizzare gli strumenti informatici, internet, la posta elettronica e gli altri servizi informatici e telematici in modo appropriato e diligente ed è responsabile della propria postazione di lavoro.

Art. 3 – Dotazioni informatiche ai dipendenti nell'ambito della modalità di lavoro a distanza.

Al dipendente in modalità di lavoro a distanza viene assegnata la seguente dotazione informatica minima:

- personal computer portatile completo di sistema operativo e software per l'accesso alla rete interna dell'Amministrazione.

Al dipendente 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

Il dipendente in modalità di lavoro a distanza accede ai servizi informatici resi disponibili dall'Amministrazione tramite le credenziali di cui all'articolo precedente, utilizza una propria postazione di lavoro virtuale, dotata di strumenti di office automation, protezione dei dati, di posta elettronica.

L'Amministrazione rende disponibile sulla postazione di lavoro virtuale gli strumenti software necessari per l'utilizzo dei servizi applicativi in un contesto di sicurezza e omogeneizzazione delle stesse postazioni di lavoro.

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

Il computer portatile o eventualmente altro device mobile eventualmente affidato al lavoratore 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.

Per evitare il 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, e in questo caso comunque su espressa autorizzazione della struttura dipartimentale competente in materia di sistemi informativi che provvederà materialmente all'installazione.

Non è consentito disinstallare o disabilitare il programma antivirus e antimalware installato; ogni eventuale malfunzionamento di quest'ultimo, va segnalato tempestivamente all'Amministrazione.

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 dal responsabile del servizio competente.

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;

È consentita esclusivamente l'installazione di supporti per la connessione mobile per l'accesso a Internet eventualmente messi a disposizione dall'Amministrazione o da essa autorizzati. Qualunque esigenza in tal senso deve essere comunicata al responsabile del servizio competente, che ha il compito di analizzare la problematica per trovare la soluzione coerente con le vigenti politiche di sicurezza e integrità della rete.

L'eventuale malfunzionamento o danneggiamento degli strumenti informatici deve essere tempestivamente comunicato al responsabile del servizio competente.

Il personale incaricato dall'Amministrazione della gestione e della manutenzione dei componenti del sistema informatico può 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.

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

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.

Laddove non diversamente previsto, la password deve essere composta da almeno 8 caratteri e formata da lettere (sia maiuscole che minuscole) e numeri e/o caratteri speciali.

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.

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.

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

In caso di cessazione del rapporto di lavoro a distanza dovrà essere cura dell'utente rimuovere ogni dato personale eventualmente presente sulle macchine in dotazione, prima che l'account individuale del dipendente sia disattivato.

Art. 7 – Protezione antivirus e antimalware

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, ecc.

Ogni utente è tenuto a controllare la presenza e il regolare funzionamento del software antivirus e antimalware eventualmente installato sul proprio computer portatile.

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 competente in materia di sistemi informativi.

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.

Art. 8 – Utilizzo delle periferiche e delle cartelle condivise

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.

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.

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.

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

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.

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 – Utilizzo di Internet

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.

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.

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

Art. 11 – Gestione e utilizzo della posta elettronica

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.

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

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.

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.

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. 13 – Aggiornamenti delle regole tecniche

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. Per quanto non specificato nel presente manuale, si fa riferimento al "Regolamento per l'utilizzo degli strumenti informatici e telematici del Comune di Verbania".