Sommario

Istruzioni e raccomandazioni

I dispositivi informatici (personal computer fissi, portatili, tablet, smartphones, stampanti multifunzione: fotocopiatrice, scanner, fax; ecc..) ed i relativi programmi e/o applicazioni affidati al dipendente sono, come è noto, strumenti di lavoro il cui utilizzo ricade sotto la responsabilità del Direttore e che possono contenere dati riservati e informazioni personali di terzi.

Vanno custoditi in modo appropriato evitando manomissioni, danneggiamenti o utilizzi, anche da parte di altre persone e possono essere utilizzati solo per fini professionali attinenti esclusivamente alle mansioni assegnate, evitando pertanto usi per fini personali, al di fuori dei casi consentiti ed autorizzati espressamente dai propri responsabili dell'Ente, tanto meno per scopi illeciti.

Debbono essere prontamente segnalati all'azienda il furto, danneggiamento o smarrimento di tali strumenti.

Le impostazioni dei dispositivi informatici sono predisposte dagli addetti informatici addetti sulla base di criteri e profili decisi dalla Direzione in funzione della qualifica del dipendente, delle mansioni cui questo è adibito, nonché dalle decisioni e della politica di utilizzo di tali strumenti stabilita dall'Azienda stessa.

Tutti gli utenti sono tenuti ad attenersi scrupolosamente alle indicazioni sotto riportate.

Utilizzo dei dispositivi informatici

- i telefoni dell'Ente, non possono essere di norma utilizzati per ricevere o effettuare comunicazioni private; si raccomanda quindi di limitare l'uso del telefono d'ufficio alle comunicazioni necessarie per lo svolgimento del lavoro, salvo casi eccezionali; il dipendente è tenuto a limitare la ricezione di telefonate personali sulle linee telefoniche dell'ufficio, avendo cura di contenere la durata delle conversazioni al minimo indispensabile;

- durante l’orario lavorativo, limitare alla gestione delle urgenze o per motivi strettamente eccezionali l’utilizzo di smartphone, tablet, ed altri device privati;

- gli utenti non devono violare o tentare di violare i sistemi di sicurezza informatici;
- gli utenti non devono né cercare di ottenere accessi non autorizzati, né favorire analoghe attività da parte di altri Utenti, interni o esterni; gli addetti non possono, deliberatamente e in modo non autorizzato, modificare o tentare di modificare dati contenuti nei Sistemi in Rete. Gli utenti non possono intercettare, tentare d'intercettare o accedere a dati in transito sulla rete aziendale, che non siano loro diretti;
- gli utenti non possono mascherare la loro identità quando usano i sistemi della rete aziendale. Gli utenti non possono inoltre impersonare altri individui;
- non è consentito installare programmi provenienti dall'esterno salvo espressa autorizzazione della Direzione; non è consentito scaricare file dalla rete o contenuti in supporti magnetici e/o ottici non aventi alcuna attinenza con la propria prestazione lavorativa;
- non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici; non è consentita l'installazione sui PC a disposizione, di mezzi di comunicazione propri;
- tutti i software caricati sul sistema operativo ed in particolare quelli necessari per la protezione dello stesso o della rete internet (quali antivirus o firewall) non possono essere disinstallati o in nessun modo manomessi dagli utenti (salvo quando questo sia richiesto dalla Direzione per compiere attività di manutenzione o aggiornamento);
- non è consentito condividere file, cartelle, hard disk o porzioni di questi del proprio computer, per accedere a servizi non autorizzati al fine di scaricare materiale elettronico tutelato dalle normative sul Diritto d'Autore (software, file audio, film, etc.);

- l'uso della Rete aziendale in violazione di norme del Codice Civile o Penale è proibito. Esempi di queste violazioni sono: distribuzione di materiale osceno; ricezione, registrazione, trasmissione o possesso d'immagini pornografiche relative a minori; violazione di copyright;
- Ogni utente è tenuto a segnalare con tempestività alla Direzione qualsiasi malfunzionamento degli strumenti informatici in uso;
- Non è consentito procedere autonomamente a tentativi di correzione di errori o malfunzionamenti, se non dietro esplicita autorizzazione della Direzione;;
- Non è permesso modificare la configurazione del proprio posto di lavoro né dal punto di vista hardware, né dal punto di vista software, senza precedente autorizzazione della Direzione. In particolare non è permesso spostare dispositivi quali unità centrali, unità video o stampanti, scanner, telefoni o fax; non è possibile modificare la configurazione dei personal computer;
- i dispositivi informatici "stand alone" o in rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo, essere utilizzate per scopi diversi.

Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità; l'azienda si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema ovvero acquisiti o installati in violazione delle presenti istruzioni.

Utilizzo dei dispositivi mobili

• L'utente è responsabile di dispositivi mobili (PC portatile, tablet, smartphone ecc) assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
• Agli stessi si applicano tutte le regole di utilizzo previste per i PC fissi o agli altri dispositivi informatici presenti in azienda.
• I dispositivi mobili utilizzati in caso di allontanamento, devono essere custoditi in un luogo protetto. In particolare essi non devono mai essere lasciati incustoditi nell'autovettura neppure nel bagagliaio.

• In caso di furto o smarrimento è obbligatorio comunicare tempestivamente l'accaduto alla Direzione, effettuare denuncia presso l'ufficio di pubblica sicurezza locale e consegnare copia della stessa in Azienda.

Gestione degli archivi, file, documenti e cartelle

• Gli archivi, file, documenti e cartelle generati e/o gestiti dagli utenti devono essere memorizzati sui dispositivi di rete. La Direzione garantisce la sicurezza delle informazioni memorizzate sui dispositivi di rete eseguendo periodici backup degli archivi.
• Non è consentita la copia di archivi dell'Ente di qualsiasi genere o specie né su dispositivi asportabili (CD,DVD, dischi o chiavi USB, tablet, smartphone e simili) né su dispositivi di memorizzazione esterni all'Azienda (ad esempio in server accessibili mediante Internet, aree dati in Cloud tipo Dropbox, Google Drive, ecc.), né via posta elettronica su account non appartenenti al dominio aziendale, se non dietro esplicita autorizzazione della Direzione.

Utilizzo di Internet

La rete internet può e deve essere utilizzata dal dipendente a supporto dell'attività lavorativa nell'ambito delle mansioni ed autorizzazioni assegnategli dal proprio responsabile.

Al fine di ridurre il rischio di un utilizzo improprio della rete e allo stesso tempo di evitare per quanto possibile controlli che potrebbero comportare il trattamento di dati personali, l'azienda si riserva di adottare l'utilizzo di sistemi e filtri che possono prevenire determinate operazioni, reputate inconferenti con l'attività lavorativa, quali ad esempio l'upload o l'accesso a determinati siti e/o il download di file o software aventi particolari caratteristiche (quali ad esempio dimensionali o di tipologia di dato), con individuazione di categorie e liste di siti cui non è concesso l'accesso (black list), in quanto non attinenti l'attività lavorativa;
Di seguito sono riportati i principi che devono essere rispettati al fine di assicurare una navigazione internet sicura:
• non è consentito lo scarico di materiale elettronico tutelato dalle normative sul Diritto d'Autore (software, file audio, film, etc.) attraverso Internet: web, ftp, servizi di condivisione, ecc.;
• non è consentita la memorizzazione di documenti di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
• è vietata ogni forma, anche a titolo personale, di registrazione a siti i cui contenuti non

Utilizzo della posta elettronica aziendale

La posta elettronica, sia interna che esterna, è un mezzo di comunicazione che il Direttore mette a disposizione del dipendente esclusivamente per consentirgli lo svolgimento della propria attività lavorativa, pertanto:

• si raccomanda di evitare di utilizzare tali strumenti per motivi non attinenti allo svolgimento delle mansioni assegnate, salvo casi eccezionali di comprovata urgenza e necessità;

• non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
• la posta elettronica diretta all'esterno della rete informatica aziendale non deve essere usata per inviare informazioni, dati o documenti di lavoro "Strettamente Riservati";
• non è consentito utilizzare caselle di posta elettronica private per corrispondenza inerente le attività dell'Ente;
• è necessario configurare un sistema di risponditore automatico da attivare in caso di prolungata assenza che avvisi il mittente dell'assenza. Si raccomanda di:
o inserire un indirizzo mail aziendale di un collega che il mittente può contattare in caso di urgenza;

Gestione delle credenziali e password

L'accesso ai dispositivi informatici, ai programmi applicativi e alle varie funzionalità messe a disposizione degli utenti per lo svolgimento dell'attività, avviene previa autenticazione, che consiste nella verifica dell'identità del dipendente attraverso l'uso di un codice identificativo e di una parola chiave (password).
Le credenziali di autenticazione sono assolutamente personali e non cedibili, per nessuna ragione.
E' necessario rispettare l'ambito di competenza (i dati cui poter accedere) ed il profilo di autorizzazione (tipi di trattamento consentito) indicate nella propria nomina ad Incaricato.
Elaborare le password seguendo le istruzioni sotto riportate.
• Al primo accesso ad un sistema e/o ad una banca dati, l'incaricato ha la responsabilità di cambiare la password assegnatagli dalla Direzione. Tale password deve essere al minimo lunga 8 caratteri, includere sia lettere, sia cifre e una maiuscola;
• la password non deve contenere elementi che possano in qualche modo essere legate all'incaricato come, ad esempio il suo nome, quello di sua moglie/marito, del cane, date di nascita, numeri di telefono etc.;
• la password non deve essere comunicata a nessuno, lo scopo principale del suo utilizzo è assicurare che nessun altro possa accedere alle risorse o sostituirsi all'incaricato;
• l'incaricato ha la responsabilità di custodire con diligenza la propria password, in nessuna circostanza il dipendente è autorizzato a condividere le proprie credenziali di autenticazione con altri addetti o terze persone;
• l'incaricato dovrà informare la Direzione nel caso in cui, abbia fondati motivi di ritenere che possa essere compromessa la riservatezza della password, o comunque che ne sia stato fatto un utilizzo indebito cambiandola immediatamente;

Custodia dispositivi informatici

I dispositivi informatici non possono essere lasciati incustoditi:
• In caso di allontanamento anche temporaneo dalla postazione di lavoro o comunque dal dispositivo informatico è necessario non lasciare il sistema aperto con la propria password.
• Al fine di evitare che persone estrne effettuino accessi non permessi; l'incaricato deve eseguire il "Log out" della sessione di lavoro o in alternativa attivare funzioni che, trascorso un breve periodo di tempo predeterminato in cui il dispositivo resta inutilizzato, non

consentino più l'accesso al dispositivo se non previa imputazione di password.
• In particolare i supporti di memorizzazione rimovibili devono essere custoditi ed utilizzati in modo tale, da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: è bene adottare archiviazioni in modo che vengano conservati in cassetti chiusi a chiave, durante il loro utilizzo, e successivamente formattati, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi;
• Una volta cessate le ragioni per la conservazione dei dati, i supporti di memorizzazione rimovibili non possono venire abbandonati. Si devono quindi cancellare i dati, se possibile, o arrivare addirittura a distruggere il supporto, se necessario.

Protezione dispositivi informatici

L'azienda adotta adeguati ed aggiornati strumenti e metodologie per la protezione dei dispositivi: segmentazione della rete, firewall, antispam, antiphising, endpoint protection (antivirus), web filtering, per i file scaricati da internet, aggiornamenti automatici di sicurezza dei sistemi operativi, backup periodici ecc.

L'incaricato è comunque tenuto ad adottare i seguenti comportamenti per prevenire danni ai sistemi, o ridurne il rischio, dall'esecuzione di software "malevolo":

• utilizzare soltanto programmi provenienti da fonti fidate. Copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato. Non utilizzare programmi non autorizzati;
• evitare la trasmissione di file eseguibili (.COM, .EXE, .OVL, .OVR) e di sistema (.SYS) tra computer in rete;
• proteggere le memoria di massa rimovibili (dischi, chiavette ecc) autorizzati da scrittura quando possibile. In questo modo è possibile evitare l'accesso e l'utilizzo da parte di software dannoso;
• non trasferire documenti, file, archivi relativi a dati dell'Ente su dispositivi non dell'Ente per essere trattati od utilizzati esternamente alla rete aziendale e riportati nella stessa;
• non aprire e non diffondere messaggi email di provenienza dubbia o con mittenti sconosciuti o con oggetto non pertinente alle proprie attività con evidenti errori ortografici o contenenti allegati o link poco chiari o dubbi, cancellandoli tempestivamente;
• nel caso di apertura di messaggi di tale tipo almeno non aprire gli eventuali allegati o non accedere ai link presenti e provvedere a eliminarli tempestivamente;
• in ogni caso, nel dubbio che ci sia in corso un'attività anomala o malevola sul proprio dispositivo, allertare immediatamente la Direzione La tempestività nell'azione di bonifica è essenziale per limitare eventuali danni arrecati al dispositivo ed ad altri dispositivi o apparati della rete aziendale;

Accesso in VPN

Per le attività di smartworking, lavoro agile e lavoro da remoto l'azienda fornisce un accesso VPN all'infrastruttura IT.

La password di accesso per la VPN è nominativa è non deve essere comunicata a terzi

Il dispositivo usato per collegarsi deve avere un antivirus installato ed attivo

Evitare di installare sul dispositivo programmi di cui non si conosce la provenienza o non necessari per l'attività aziendale

Evitare di navigare su siti sconosciuti o sospetti che potrebbero installare sul device codice malevole

Utilizzo di dispositivi ICT privati

. E' possibile utilizzare dispositivi privati quali PC, Tablet, Smartphone, ecc. unicamente per la fruizione dei servizi informatici dell'Ente disponibili su internet ed utilizzando le credenziali di accesso fornite.

Non è consentito il collegamento alla rete aziendale di dispositivi privati se non preventivamente richiesto ed autorizzato dal Direttore.

L'utente è consapevole che l'uso promiscuo del dispositivo per attività personali e professionali/dell'Ente comporta il rispetto delle disposizioni e delle raccomandazioni di seguito indicate.

Nell'utilizzo di dispositivi privati per accedere alla rete aziendale non sono tollerati i seguenti comportamenti:

• in modo illecito o abusivo accedere, modificare, danneggiare, distruggere informazioni, dati e sistemi informatici o telematici;

• in modo illecito o abusivo, diffondere, installare, elaborare, conservare, trasferire materiale che consenta di accedere, modificare, danneggiare, distruggere le comunicazioni informatiche;

• installare, elaborare, conservare, trasferire materiale pornografico in genere, nonché programmi, documenti, immagini, materiali audio e video o informazioni di vario tipo che offendano il pubblico pudore o che siano diffamatori, osceni, indecenti o lesivi della dignità umana;

• falsificare documenti informatici pubblici o privati;

• diffondere virus o malware. A tal scopo è considerata diretta responsabilità dell'utilizzatore provvedere a dotarsi di sistemi di sicurezza informatica quali antivirus, spamming, malware, ecc.

Il dispositivo deve essere dotato dei seguenti strumenti di protezione:

• protezione di accesso: attraverso password e/o impronta biometrica;

• protezione della SIM di telefonia: attraverso PIN;

• protezione dei supporti di memorizzazione: l'hard disk interno e gli eventuali supporti di memorizzazione rimovibili quali microSD card, devono essere protetti all'accesso tramite pin o password in modo da evitare accessi indesiderati in caso di smarrimento o furto;

• L'utente non deve tenere dati dell'Ente salvati sul proprio dispositivo personale

• Evitare l'accesso ai servizi dell'Ente attraverso dispositivi di cui non si conosce la provenienza o forniti da Internet Point o terzi;

• verificare preventivamente la presenza ed il funzionamento di un prodotto antivirus installato sul dispositivo dal quale si accede;

• porre la massima attenzione nella digitazione delle proprie credenziali di accesso per evitare che qualcuno possa impossessarsene;

• non salvare, per memoria, nel dispositivo privato le credenziali di accesso;

• chiudere sempre la sessione di collegamento;

• non installare App e programmi da siti e store non ufficiali;

• non utilizzare dispositivi dove è stato sbloccato il meccanismo di protezione della distribuzione software (Jailbreak)

Controlli dell'Ente

L'Ente, quale datore di lavoro, fermo restando il divieto di monitoraggi sistematici e costanti, può effettuare periodicamente controlli ed ispezioni, anche a garanzia della sicurezza e riservatezza dei dati personali oggetto di trattamento. L'Ente, quale datore di lavoro, si riserva la facoltà di accedere in qualsiasi momento, nel rispetto della normativa sulla privacy e del presente regolamento, a tutti gli strumenti informatici, telematici e telefonici dell'Ente assegnati in dotazione ai singoli utenti per l'espletamento delle proprie mansioni lavorative, ai documenti e ai dati personali e alle altre informazioni ivi contenute.
Resta inteso che L'Ente si astiene da qualsiasi finalità di controllo sistematico dell'attività lavorativa (vale a dire dal compimento di controlli prolungati, continuativi, intenzionalmente ad elevata frequenza).
Nell'espletare controlli e verifiche le funzioni interne preposte devono garantire la massima riservatezza dei dati conosciuti, anche incidentalmente, in occasione della verifica, pena l'applicazione di sanzioni disciplinari in base alla gravità dell'accaduto. Le informazioni derivanti dai controlli potranno quindi essere rese disponibili solo ed esclusivamente a soggetti interni o esterni alla Società per cui la comunicazione sia necessaria in relazione alle finalità perseguite con l'accesso, comunque nel rispetto dei principi di correttezza, necessità, pertinenza e non eccedenza previsti dalla legge.
I controlli potranno essere collettivi (es. rete aziendale, funzionamento della posta elettronica) oppure su singoli dispositivi o postazioni o utenti e avverranno, più spesso, in caso di anomalie o abusi (spot o reiterati).
Oltre a ciò l'Ente si riserva di effettuare specifici controlli sui software e/o applicazioni caricati sui dispositivi informatici dell'Ente utilizzati dagli addetti, al fine di verificarne la regolarità sotto il profilo delle autorizzazioni e delle licenze, nonché, in generale, la conformità degli stressi alla Normativa vigente e di effettuare specifici controlli ad hoc nel caso di segnalazioni di attività che hanno causato danno o che ledono diritti di terzi o che comunque sono illegittime.
I controlli potranno avere luogo con o senza preavviso. Il preavviso potrà essere collettivo od individuale, e sarà comunicato all'utente nel rispetto del principio di gradualità, di cui meglio oltre.
Nei casi in cui sia necessario restringere l'ambito della verifica, l'azienda si riserva di poter protrarre l'indagine fino all'individuazione puntuale del singolo utente, secondo il principio di "Graduazione dei controlli" enunciato al punto 6.1(8) in premessa al provvedimento del Garante: "le linee guida del Garante per posta elettronica e internet" – (Gazzetta Ufficiale n. 58 del 10 marzo 2007):

In caso di anomalie, il personale effettuerà controlli che si concluderanno con avvisi e richiami generalizzati diretti a tutti i soggetti dell'area o del settore o altra unità organizzativa in cui si è rilevata l'eventuale anomalia:

Ulteriori controlli aventi base individuale potranno avvenire:
a) in caso di ulteriori e anomalie o abusi successivi/ all’avviso precedente, o comunque
b) anche fin dall'inizio, nel caso in cui, sulla base degli elementi conoscitivi disponibili, il Direttore abbia ragionevole motivo di sospettare che l'utilizzo degli strumenti dell’Ente da parte del singolo individuo, in assenza di immediati specifici controlli possa arrecare un pregiudizio anche solo potenziale alla stessa (controlli aventi scopo cd. "difensivo") e/o determinare eventi che le finalità stesse del controllo mirano a prevenire od a contrastare.