MODELLO DI ORGANIZZAZIONE
GESTIONE E CONTROLLO

ALL. "D"

REGOLAMENTO INTERNO PER L'UTILIZZO DEL SISTEMA INFORMATIVO AZIENDALE

Approvato
dall'Organo Amministrativo
con Delibera n° 01 in data 11.03.22

Associata a federcasa
Via del Villone n. 4 - 51100 Pistoia - Tel. 0573/50421 – Fax 0573/32644 – C.F. - P.I. - n. R.I. 01530000478
Cap.Soc. € 750.000,00 i.v. - n. R.E.A. 157386 Sito internet: www.spesweb.it e-mail: info@spesweb.it

1. Introduzione

1.1. Scopo e norme applicabili

Questo documento definisce le norme e le procedure a cui obbligatoriamente dovranno attenersi tutti gli utenti – a qualsiasi titolo – del sistema informativo aziendale. Una volta sottoscritto, ne vige l'obbligo di osservanza da parte di tutto il personale e di tutte le funzioni aziendali, in conformità tra l'altro alle seguenti disposizioni cogenti:

Le disposizioni di cui al Codice in materia di protezione dei dati personali (D. Lgs. 196/2003), comprese le statuizioni contenute nel suo Allegato B;

Le disposizioni di cui al Provvedimento del Garante per la protezione dei dati personali del 01.03.07 "Lavoro: le linee guida del Garante per posta elettronica e Internet" pubblicato in Gazzetta Ufficiale n. 58 del 10.03.07 (di seguito le "Linee Guida");

Il D. Lgs 81 / 2008 in materia di sicurezza sul lavoro;

Il D. Lgs 231 / 2001 in materia di responsabilità amministrativa degli enti;

La legge 300/1970

1.2 Ambito di applicazione

Il presente disciplinare si applica a chiunque, a qualunque titolo (ad esempio rapporto di lavoro subordinato, rapporto di collaborazione, consulenza etc.), di seguito definito anche "Utente", utilizzi, per finalità connesse con l'esercizio dell'attività lavorativa, beni aziendali quali, in particolare, strumenti informatici (Personal Computer, Tablet, Telefoni Cellulari, Smartphone) nonché tutta la dotazione informatica relativa (hardware, software, rete aziendale, caselle di posta elettronica etc.)

Il presente documento si applica in tutte le sedi aziendali di SPES s.c.r.l. e al di fuori di esse quando si utilizzino beni aziendali.

2. Disposizioni in merito agli obblighi degli Utenti

Gli Utenti, come definiti al paragrafo 1.2., dovranno osservare gli obblighi descritti nelle indicazioni generali di seguito riportate.

I sistemi informatici, le reti aziendali e le postazioni di lavoro (Personal Computer) utilizzati da ogni Utente sono di proprietà di SPES la quale stabilisce le misure tecniche ed organizzative per assicurare la riservatezza, l'integrità e la disponibilità delle informazioni in accordo con le disposizioni della legislazione esistente e nell'assoluto rispetto delle normative sulla sicurezza e riservatezza dei dati.

L'utilizzo degli strumenti definiti più sopra è limitato esclusivamente all'attività lavorativa definita dall'azienda e, pertanto, qualsiasi uso personale è vietato. Tale divieto si estende anche all'utilizzo dei software accessibili per scopi lavorativi, ivi inclusa la posta elettronica, che devono essere esclusivamente adibiti alla trasmissione di comunicazioni e file aziendali e relativi alle mansioni svolte, nonché all'accesso e navigazione in Internet.

2.1. Norme relative al corretto utilizzo dei PC

2.1.1. Il PC (Personal Computer) affidato all'Utente è uno strumento di lavoro e questi è responsabile del suo utilizzo. Ogni utilizzo non inerente l'attività lavorativa può contribuire a generare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

2.1.2. Non è consentito all'Utente di modificare le caratteristiche hardware e software del proprio PC, salvo preventiva autorizzazione esplicita da parte del responsabile Ufficio CED. In particolare non è consentito installare alcun software senza preventiva autorizzazione, anche se inerente l'attività aziendale o si tratti di aggiornamenti di software già presenti sul PC.

2.1.3. Le informazioni archiviate elettronicamente nella memoria di massa (Disco Rigido) del PC o dei Server di rete devono essere esclusivamente quelle necessarie all'attività lavorativa.

2.1.4. Costituisce buona regola la pulizia periodica degli archivi, da eseguirsi almeno ogni 6 (sei) mesi, con cancellazione dei file obsoleti o inutili. Particolare attenzione va prestata alla duplicazione dei dati, al fine di evitare un'archiviazione ridondante.

2.1.5. La tutela della gestione locale di dati su stazioni di lavoro personali – PC che gestiscono localmente documenti e/o dati – è demandata all'Utente che dovrà effettuare, con frequenza opportuna, i salvataggi sul server di rete.

2.1.6 Inoltre, gli Utenti dei sistemi di proprietà di SPES sono tenuti a:

- ✓ utilizzare solamente software e periferiche approvati dall'Ufficio CED. Nel caso in cui si renda necessario un software e/o periferica specifica, deve essere contattato il Responsabile CED per l'autorizzazione;
- ✓ eseguire le misure di sicurezza per garantire la protezione dei propri strumenti di lavoro e la sicurezza della propria postazione di lavoro.
- ✓ effettuare il log out dal proprio PC al termine della giornata lavorativa;
- ✓ nel caso la postazione di lavoro sia lasciata incustodita impostare il bloccaggio dello schermo (da sbloccare tramite password) o effettuare il log out;
- ✓ al termine dell'orario di lavoro:
- per quanto possibile evitare che documenti cartacei contenenti informazioni e dati personali di terzi rimangano incustoditi e conservarli in appositi cassetti o armadi;

Le seguenti attività sono espressamente proibite:

- ✓ distruggere, modificare, disabilitare, copiare (in caso di software od applicativi) o danneggiare gli strumenti informatici di proprietà di SPES, i dati, i programmi e i documenti elettronici contenuti nella rete aziendale e nelle copie di sicurezza (backup);
- ✓ ostacolare intenzionalmente l'accesso di altri Utenti alla rete attraverso un utilizzo eccessivo delle risorse IT e della connettività aziendale o compiere azioni che danneggino, interrompano o creino errori nei sistemi;
- ✓ tentare di aumentare il livello di privilegi dell'Utente nei sistemi;
- ✓ l'uso di dispositivi digitali propri connessi alla rete aziendale;
- ✓ utilizzare e/o installare modem di qualsiasi tipo (ad es. RTC, RDS, xDSL, GSM, 3G, 4G, LTE) sui PC connessi alla rete aziendale;
- ✓ installare programmi, virus, macro, applet, controlli ActiveX od ogni altro dispositivo/software logico o stringhe di caratteri che causino, o possano causare, un cambiamento indesiderato nei sistemi aziendali o di terze parti;
- ✓ installare/effettuare download di software/applicativi non autorizzati;
- ✓ eliminare un programma o file installato legalmente in modo tale da impedire od ostacolare le normali operazioni, ivi inclusa la disattivazione dei sistemi di sicurezza;
- ✓ scaricare ed archiviare applicativi/file personali nelle cartelle presenti nella rete aziendale.

2.2. Norme di comportamento relative all'accesso alla rete aziendale e alla rete Internet

2.2.1. L'accesso alla rete intranet aziendale e di conseguenza alla rete Internet avviene esclusivamente tramite un codice identificativo personale (user-id) e una parola chiave individuale (password); l'Utente è tenuto a conservare con la massima cura e segretezza la password di accesso alla rete ed ai sistemi (la password deve essere nota solo all'Utente e non può essere condivisa con altre persone) e a scollegarsi (logout) al termine della sessione di lavoro e/o in caso di assenze dall'ufficio per un prolungato periodo di tempo. In questi casi, al fine di assicurare la disponibilità per l'azienda dei detti dati e/o degli strumenti elettronici, in caso di prolungata assenza dell'Utente o di un suo impedimento, l'accesso agli strumenti elettronici affidati all'Utente sarà effettuato dall'Ufficio CED, che informerà tempestivamente l'Utente stesso circa l'intervento effettuato

2.2.2. La password di accesso alla rete locale:

- scade ogni tre mesi;
- è diversa dalla user-id;
- è costituita almeno di otto (8) caratteri.

Le istruzioni per costruire password non facili da individuare sono fornite dall'Ufficio CED.

2.2.3. In accordo con la vigente normativa sulla protezione dei dati – in particolare con quanto disposto dall'All. B del D. Lgs 196/2003 – nonché con le politiche di sicurezza di SPES vigenti e i ruoli aziendali presenti, sono definiti i profili di autorizzazione dell'Utente per l'accesso agli elaboratori e ai dati, e si effettua l'associazione utente – profilo di autorizzazione.

2.2.4. E’ assolutamente proibita la navigazione Internet per motivi diversi da quelli strettamente legati all’attività lavorativa stessa.
2.2.5 E’ assolutamente proibita in particolare la navigazione Internet in siti ritenuti insicuri, pedopornografici, politici, etc; SPES può attivare un sistema di filtri che prevengono determinate operazioni – reputate incoerenti con l’attività lavorativa – quali l’upload o l’accesso a determinati siti (inseriti in una blacklist) e/o il download di file o software aventi particolari caratteristiche (dimensionali o di tipologia di dato).
2.2.6 In riferimento al punto precedente è espressamente proibito anche l'accesso e l'utilizzo di servizi cloud per l'archiviazione di dati (storage) quali (solo a titolo di esempio) Google Docs o Dropbox, nonché di servizi di webmail (posta elettronica via web) quali (solo a titolo di esempio) Gmail, Yahoo Mail, Hotmail.
2.2.7. Non è consentito utilizzare abbonamenti Internet privati per collegamenti alla rete Internet.
2.2.8. La non ottemperanza delle suddette norme determinerà l’attuazione da parte dell’azienda di restrizioni considerate appropriate, nonché di provvedimenti disciplinari laddove applicabili.
2.2.9 L'accesso agli archivi presenti nelle cartelle esistenti nel server di rete è consentito secondo le autorizzazioni concesse ai diversi uffici dall'Ufficio CED, salve autorizzazioni individuali diverse concesse dalla direzione, per iscritto.

2.3. Norme di comportamento relative all’utilizzo della posta elettronica
2.3.1. L’indirizzo di posta elettronica sul dominio aziendale fornito all’Utente costituisce uno strumento di lavoro e dovrà, pertanto, essere utilizzato esclusivamente per l’espletamento delle attività lavorative. Ciascuno ne è responsabile come di qualsiasi altra dotazione.
Ogni utilizzo non inerente l’attività lavorativa può contribuire a generare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Non è consentito configurare o utilizzare altri account di posta elettronica diversi da quello assegnato o account webmail di ogni tipo.
2.3.2. Ogni Utente deve usare estrema cautela nella ricezione degli allegati inviati da fonti sconosciute.
2.3.3. Sono in ogni caso proibite le seguenti attività:

- ✓ invio di messaggi e/o allegati non inerenti a scopi professionali, che interferisca con i processi di comunicazione del Personale od interrompa le normali operazioni della rete aziendale;
- ✓ falsificazione e/o modificazione di messaggi e-mail;
- ✓ lettura, copia o modifica di messaggi e-mail o file di altri Utenti senza il loro consenso, sia per ottenere informazioni riservate o violare la loro privacy, sia per appropriazione od intercettazione dei loro messaggi anche per mezzo di strumenti d’intercettazione audio, registrazione immagini od ogni altro mezzo di comunicazione;
- ✓ invio o inoltro improprio di messaggi del tipo a catena o piramidale;
- ✓ apertura di file di dubbia origine senza prima consultare il personale responsabile;
- ✓ invio di messaggi od immagini di natura illegale, offensiva, diffamatoria, inappropriata o con contenuto discriminatorio riguardo al genere, età, sesso, inabilità o materiale che promuova molestie sessuali o la pornografia;
- ✓ utilizzo della rete aziendale per la partecipazione a giochi, lotterie ed aste, per il download di video, audio od altro materiale non strettamente correlato all’attività lavorativa.

2.3.4. La non ottemperanza delle suddette norme determinerà l’attuazione da parte dell’azienda di restrizioni considerate appropriate, nonché di provvedimenti disciplinari laddove applicabili.
2.3.5 L'accesso alle caselle di posta aziendali è consentito solo ed esclusivamente per mezzo dei programmi software autorizzati dall'Ufficio CED, sia sui PC che sui dispositivi mobili.
2.3.6 E’ da evitare l’invio di messaggi con allegati di grosse dimensioni. Se l’invio è necessario occorre informare l'Ufficio CED.

2.4. Norme ulteriori riguardanti l’utilizzo dei PC portatili e dei dispositivi mobili (tablet e smartphone)
2.4.1. L’Utente è responsabile del dispositivo assegnatogli dall’azienda e deve custodirlo con diligenza sia durante gli spostamenti che durante l’utilizzo nel luogo di lavoro.
2.4.2. Ai dispositivi di oggetto del presente paragrafo si applicano le regole di utilizzo previste per i PC da scrivania, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
2.4.3. I dispositivi utilizzati all’esterno delle sedi aziendali (convegni, visite presso fornitori e/o clienti, etc.) in caso di allontanamento, devono essere custoditi in un luogo protetto.

2.4.4. Nel caso di accesso alla rete aziendale tramite Accesso Remoto o VPN è fatto obbligo di utilizzare l'accesso in forma esclusivamente personale e utilizzare la password in modo rigoroso. Al termine della sessione di lavoro è sempre necessario disconnettersi.
2.4.5. Non è consentito utilizzare abbonamenti Internet privati per collegamenti alla rete Internet.

3. Controlli da parte dell'azienda
3.1. L'Azienda si riserva la facoltà di effettuare controlli occasionali per verificare l'integrità del sistema informativo, per l'ordinaria manutenzione dello stesso e per ottemperare a disposizioni di legge come ad esempio attuare le misure di controllo previste dal modello di gestione di cui al D. Lgs. 231/2001, riservandosi, in tale sede, di accertare e segnalare tempestivamente eventuali abusi commessi dall'Utente.

Per le suddette ragioni, SPES si riserva di monitorare le reti ed i sistemi aziendali nei seguenti casi:
- necessità di effettuare verifiche sulla funzionalità e sulla sicurezza dei sistemi;
- constatazione di utilizzo indebito della posta elettronica e della rete Internet;
- presenza di casi di abusi da parte di singoli o reiterati;
- presenza di indizi relativi alla fuga di informazioni riservate o confidenziali.

Le informazioni relative ai file di log verranno trattate esclusivamente dall'Ufficio CED e dalla Direzione. Nei file di log relativi all'utilizzo della rete Internet sono contenuti l'indirizzo della postazione di lavoro o del dispositivo utilizzato, l'indirizzo web o IP di destinazione (per esempio il sito visitato) e le informazioni temporali relativi alla connessione.
I controlli verranno effettuati preventivamente su informazioni appartenenti a gruppi collettivi di Utenti, tramite l'analisi di statistiche generali. Successivamente verranno inoltrati avvisi collettivi di diffida al compimento di operazioni non consentite o, a seconda della gravità, verranno prese misure di tipo individuale, specialmente in caso di abuso e/o anomalie reiterate. I dati relativi ai file di log del firewall verranno conservati per un periodo di sei mesi e funzionalmente alla capienza dei server. Nei casi in cui si debba far fronte a particolari esigenze tecniche o di sicurezza oppure si debbano utilizzare tali dati rispetto all'esercizio od alla difesa di un diritto in sede giudiziaria, oppure si ottemperi all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria, tale periodo di conservazione verrà debitamente prolungato. In ogni caso verranno esclusi controlli prolungati, costanti o indiscriminati o comunque preordinati al controllo a distanza dei lavoratori.

A tal fine si specifica che:
In ogni caso non si fa luogo alla lettura e alla registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail. SPES, inoltre, non procede alla riproduzione o memorizzazione sistematica delle pagine web visualizzate dall'Utente, né alla lettura e alla registrazione dei caratteri inseriti tramite tastiera o analogo dispositivo né all'analisi occulta dei computer portatili affidati in uso.

3.2. L'Ufficio CED può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza, sia sul PC degli Utenti che sulle unità di rete.
3.3. L'effettuazione di tali controlli, che non hanno lo scopo di monitorare l'attività dell'Utente, ma bensì di verificare la sicurezza del sistema e di effettuare la manutenzione, avverranno nel pieno rispetto della privacy dello stesso e delle regole sul corretto trattamento dei dati personali che dovessero essere gestiti dall'Azienda.

3.4. Di tali controlli indiretti e del relativo trattamento dati verrà data informativa all'Utente in base all'art. 13 del D. Lgs. 196/2003; l'eventuale conservazione di tali dati avverrà per il tempo strettamente limitato al perseguimento lecito di finalità organizzative, produttive e di sicurezza.
3.5. Ogni Utente deve tenere comportamenti tali da ridurre il rischio di attacchi al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo (malware), nonché di spamming (posta elettronica indesiderata): pertanto è obbligatorio controllare la presenza ed il regolare funzionamento del software antivirus aziendale e sospendere l'attività nel caso di segnalazione di virus, avvertendo il responsabile del proprio Ufficio o l'Ufficio CED.

3.6. Il mancato rispetto o la violazione delle regole contenute nel presente disciplinare interno è perseguibile con provvedimenti disciplinari ed altresì con le azioni civili e penali previste dalle leggi vigenti, qualora si verifichino gli estremi per la sussistenza della responsabilità civile o penale.

4. Osservanza delle disposizioni in materia di privacy

E', in ogni caso, obbligatorio attenersi alle disposizioni in materia di privacy e protezione dei dati, in particolare per quanto attiene alle misure minime di sicurezza così come descritte nella lettera di nomina a Incaricato o Responsabile del trattamento dei dati.

5. Aggiornamento e revisione

Tutti gli Utenti possono proporre, quando lo ritengono necessario, integrazioni al presente disciplinare interno. Le proposte verranno esaminate dalla Direzione. Il presente disciplinare interno è soggetto a revisione con frequenza annuale.