CALORE VERDE S.r.l.

USO DEI SISTEMI INFORMATICI

Ed. dicembre 2023

1. SCOPO

Scopo della presente procedura è disciplinare l'uso dei sistemi informatici della società da parte degli utenti al fine di

a) Perseguire il rispetto delle normative vigenti in materia e la ragionevole prevenzione delle ipotesi di reato previste dal d. lgs. n. 231/2001;
b) Garantire la sicurezza dei sistemi informatici della società.

2. AMBITO

La presente procedura ha ad oggetto l'utilizzo dei sistemi informatici della Società.

Il Proto si rivolge a tutti gli Utenti e Amministratori di Sistema.

3. DEFINIZIONI

Si definisce "sistema informatico" un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate - per mezzo di un'attività di "codificazione" e "decodificazione" - dalla registrazione o memorizzazione, per mezzo di impulsi elettronici, su supporti adeguati, di dati, cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit), in combinazione diverse, e dalla elaborazione automatica di tali dati, in modo da generare informazioni, costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente. (Cass. pen., sez. VI 14-12-1999 (C.C. 04-10-1999), n. 3067). "Sistema telematico" si ha quando l'elaboratore è collegato a distanza con altri elaboratori.

Per "utente" si intende chiunque al quale sia assegnato in uso un sistema informatico dalla Società, ovvero che abbia accesso alla reti informatica aziendale o a dati, informazioni o programmi pertinenti ad un s.i. o alla rete aziendale.

Per "profilo" si intende l'insieme delle autorizzazioni e facoltà concesse dalla Società inerenti all'accesso e/o all'utilizzo di sistemi informatici o telematici, ovvero di reti informatiche interne (es. intranet) o esterne (es. internet) o di programmi, registri, archivi, banche dati della Società o di terzi.

4. PRINCIPI GENERALI

Lo svolgimento dell'attività in ambito deve improntarsi al rispetto delle vigenti disposizioni di legge (in particolare, quelle a tutela dei dati personali), nonché dei principi e delle misure di prevenzione dei reati e dei fenomeni corruttivi.

La società è in possesso di sistemi informatici (computer, server, reti LAN e wireless, connessioni di linea, routers, ecc…), comprensivi di hardware e software regolarmente licenziati, concessi in uso agli utenti con lo scopo esclusivo di adempiere alle proprie obbligazioni nei confronti della Società in relazione al perseguimento dell'oggetto di quest'ultima. Il loro utilizzo è, quindi, consentito nei limiti di tali finalità.

Tutti i software installati nei sistemi della società sono e devono essere regolarmente licenziati ed il loro uso si attiene ai limiti delle licenze. Della conservazione della documentazione comprovante la legittimità dell'uso dei software installati è responsabile l'amministratore di sistema; copia delle licenze è conservata presso l'amministrazione. L'installazione dei software è riservata all'amministratore di sistema ed è fatto divieto agli utenti di eseguire tali operazioni.

Ogni utente è personalmente responsabile dell'integrità (fisica e funzionale) dei sistemi medesimi, dei dati, delle informazioni e dei programmi ad essi relativi, ed è quindi tenuto ad aggiornare, ove richiesto, i sistemi di protezione (antivirus, firewall, ecc…) dei sistemi in utenza.

L'accesso ad ogni singolo sistema informatico e telematico è limitato ad uno o più utenti identificati, attraverso la sorveglianza dei locali ed il ricorso a chiavi fisiche (le porte di accesso ai locali sono chiuse a chiave) e logiche (user ID e password). Queste ultime appartengono in ogni caso (anche quando modificate dall'utente) alla società.

Ad ogni User-ID corrisponde un profilo di accesso ai sistemi informatici ed alle reti aziendali e a internet. Ad ogni profilo corrispondono l'utilizzo concesso degli applicativi, il limite di accesso al sistema informativo aziendale e le attività consentite (visualizzazione, inserimento dati, modificazione dei dati inseriti). Le User-ID sono assegnate unicamente su disposizione dell'A.U.

Qualora un utente sia in possesso di chiavi di accesso a s.i. non della Società, che egli debba utilizzare nell'ambito delle attività svolte per conto della Società, l'utente è tenuto a:

1) conservare le chiavi di accesso con modalità tali da non consentire a soggetti non autorizzati di venirne a conoscenza;
2) fare uso delle chiavi di accesso nei limiti delle autorizzazioni concesse;
3) non appena vengano meno le ragioni per le quali le autorizzazioni di accesso a s.i. esterni siano state concesse, dare comunicazione al terzo concedente della circostanza, e restituire ovvero annullare le chiavi di accesso;
4) dare informazione all'A.U., del possesso di tali chiavi, del titolare esterno di tali chiavi, delle ragioni per le quali esse siano state concesse.

Sarà cura della Società dare comunicazione al terzo concedente della circostanza sub 3), affinché questi assuma i provvedimenti conseguenti.

L'uso di posta elettronica attraverso le caselle con dominio o account aziendale è ad esclusivo scopo istituzionale e mai personale. La posta elettronica in entrata ed in uscita da detta caselle deve intendersi come diretta ed inviata da una funzione aziendale e come tale, essa è accessibile ai superiori dell'Utente.

E' consentito agli utenti accedere ad una casella di posta elettronica ad uso personale su web.

Gli utenti, durante i periodi di assenza, sono tenuti a predisporre messaggi di risposta automatici con i quali si avvisano i mittenti di messaggi di posta elettronica alla casella con dominio aziendale, che questi sono stati ricevuti, ma che non potranno essere letti sino al rientro dell'utente assente e che, pertanto, in caso di urgenza essi dovranno essere inviati nuovamente all'indirizzo del rispettivo responsabile di funzione e/o di progetto.

L'accesso alla rete internet potrà essere limitato mediante ricorso a black list di siti vietati.

E' vietato qualsiasi uso dei sistemi informatici per scopi incompatibili con quello per il quale essi sono concessi in uso agli utenti. In particolare è vietato:

- l'uso ludico dei sistemi informatici;
- operare il download, il caricamento o l'installazione di software (musicali, film, foto, programmi, ecc…) non autorizzati e, comunque, in violazione del diritto d'autore;

- rendere in qualsiasi modo noto a terzi non autorizzati, o comunque consentire a questi la conoscenza di dati, informazioni, formule, descrizioni di processi, documenti, materiale di qualsiasi natura, coperto da riservatezza o la cui conoscenza da parte di soggetti terzi potrebbe recare danno alla società o a terzi;
- produrre, detenere, diffondere, in qualsiasi forma e modo, materiale pornografico, pedopornografico, di propaganda od istigazione a fini terroristici, ovvero offensivo dell'onore o dignità di terzi, o comunque in violazione di legge;
- compiere azioni dirette o strumentali a violare abusivamente s.i., registri o archivi informatici della società di terzi, e/o falsificare dati, informazioni o documenti informativi di qualsiasi specie;
- porre in essere una delle condotte previste dal d. lgs. 231/2001, ed in particolar modo dall'art. 24bis, ovvero anche altra condotta strumentale alle medesime.

E' altresì vietato, a meno che non sia specificatamente ed espressamente autorizzato, l'utilizzo per scopi personali non ricompresi in quelli sopra elencati.

L'uso dei videoterminali deve essere compiuto in conformità alle prescrizioni del d. lgs. 81/2008.

I disegni, i dati e le informazioni relativi alle commesse, al personale, ai clienti e/o ai fornitori, i registri amministrativi, i libri sociali, i dati e le informazioni sulle condizioni economiche, patrimoniali e/o finanziarie della società hanno carattere riservato e non possono essere divulgati a terzi non aventi diritto, né essere usati per scopi diversi dall'esecuzione delle mansioni assegnate.

La Società esegue il back up delle informazioni trattate con i s.i. onde consentire la conservazione degli archivi informatici per il tempo previsto dalle norme vigenti.

Nei limiti della normativa vigente a tutela dei dati personali, della dignità e della riservatezza del lavoratore[1], la Società compie controlli difensivi, direttamente sui sistemi informatici in uso ai dipendenti, in presenza di un fondato sospetto di un illecito, al fine di verificarne la commissione.

Sarà cura dell'A.U. conservare le evidenze di ciò che giustifica il fondato sospetto e del momento in cui esso è sorto[2].

---

[1] A fini meramente indicativi, si dà atto di alcuni principi di diritto affermati dalla Corte di Cassazione: "Sono consentiti i controlli anche tecnologici posti in essere dal datore di lavoro finalizzati alla tutela di beni estranei al rapporto di lavoro o ad evitare comportamenti illeciti, in presenza di un fondato sospetto circa la commissione di un illecito, purché sia assicurato un corretto bilanciamento tra le esigenze di protezione di interessi e beni aziendali, correlate alla libertà di iniziativa economica, rispetto alle imprescindibili tutele della dignità e della riservatezza del lavoratore, sempre che il controllo riguardi dati acquisiti successivamente all'insorgere del sospetto" (…) "elementi, evidentemente utili anche ad orientare il bilanciamento del giudice italiano nei casi di controlli difensivi "in senso stretto", sono: i) l'informazione del lavoratore circa la possibilità che il datore di lavoro adotti misure di monitoraggio, con la precisazione che la stessa dovrebbe, in linea di principio, essere chiara sulla natura della sorveglianza ed essere precedente alla sua attuazione; ii) il grado di invasività nella sfera privata dei dipendenti, tenendo conto, in particolare, della natura più o meno privata del luogo in cui si svolge il monitoraggio, dei limiti spaziali e temporali di quest'ultimo, nonché del numero di persone che hanno accesso ai suoi risultati; iii) l'esistenza di una giustificazione all'uso della sorveglianza e alla sua estensione con motivi legittimi, con la precisazione che quanto più invadente è la sorveglianza, tanto più gravi sono le giustificazioni richieste; iv) la valutazione, in base alle circostanze specifiche di ciascun caso, se lo scopo legittimo perseguito dal datore di lavoro potesse essere raggiunto causando una minore invasione della vita privata del dipendente; v) la verifica di come il datore di lavoro abbia utilizzato i risultati della misura di monitoraggio e se siano serviti per raggiungere lo scopo dichiarato della misura; vi) l'offerta di adeguate garanzie al dipendente sul grado di invasività delle misure di sorveglianza, mediante informazioni ai lavoratori interessati o ai rappresentanti del personale circa l'attuazione e l'entità del monitoraggio, dichiarando l'adozione di tale misura a un organismo indipendente o mediante la possibilità di presentare reclamo" (Cass. Civ. sez. lav. - 26/06/2023, n. 18168)

[2] "Non può dubitarsi che incomba sul datore di lavoro l'onere di allegare prima e provare poi le specifiche circostanze che lo hanno indotto ad attivare il controllo tecnologico ex post, considerato che solo tale

Con specifico riguardo alla posta elettronica, nel caso di assenza programmata, l'utente può indicare con comunicazione scritta all'A.U. un dipendente suo fiduciario, per l'apertura della posta elettronica destinata all'account personale. In tal caso l'accesso alla posta elettronica è consentito esclusivamente a quest'ultimo.

La corrispondenza con l'O.d.V. e con il RPC è sempre riservata e non potrà essere aperta, né visionata, se non da costoro.

Chi svolge operazioni di tutela o di controllo è tenuto a conservare il riserbo e a non divulgare a terzi le informazioni o dati, riservati, ovvero personali, relativi all'utente o terze persone delle quali vengano a conoscenza nel corso delle operazioni effettuate, purché non siano esse stesse pertinenti ad un reato, ovvero ad un illecito ai sensi del codice disciplinare della società. Le informazioni raccolte nel corso delle operazioni di controllo, o comunque lecitamente apprese anche casualmente dalla Società, possono essere utilizzate nell'ambito di procedimenti disciplinari a norma del codice disciplinare della Società, ovvero per la tutela giurisdizionale della Società o di terzi, davanti a corti nazionali o estere o arbitrati di qualsiasi specie.

La società può revocare, in tutto o in parte, l'uso dei sistemi informatici, ovvero impedire, in tutto o in parte, l'accesso ad internet ad uno o più utenti (p.es. facendo uso di filtri). I poteri di revoca e le politiche di limitazione all'uso dei sistemi informatici e telematici (accesso alle reti internet ed intranet, all'uso della posta elettronica, ecc…) spettano all'A.U..

Con la sottoscrizione della presente procedura, tutti gli utenti accettano espressamente ed aderiscono alle prescrizioni contenute nella presente procedura, comprese quelle concernenti l'utilizzo dei sistemi informatici e quelle relative agli accessi ai medesimi ed ai dati e alle informazioni ad essi pertinenti, nonché all'uso di tali dati ed informazioni, nei limiti qui specificati.

5. PRINCIPI DI CONDOTTA

I profili e l'uso dei sistemi informatici sono assegnati su disposizione dell'A.U. che verifica la compatibilità con le mansioni assegnate e la presenza di eventuali precedenti disciplinari, dietro richiesta del responsabile di funzione o di commessa. I profili assegnati sono registrati e conservati dall'amministratore di sistema e dell'amministrazione della società.

I sistemi informatici sono concessi in uso mediante consegna da parte dell'amministratore di sistema di "User-Id" e password di accesso al sistema e alle utilities protette (sap, intranet, ecc..). Le password sono conservate dall'amministratore di sistema e dell'amministrazione. Costoro provvedono alla conservazione delle stesse con modalità tali da non consentire a terzi non autorizzati di venire a conoscenza delle password. Le password e le ID appartengono in ogni caso alla Società.

Le password non potranno essere cambiate fino alla loro scadenza. Alla scadenza si opererà allo stesso modo.

L'uso dei s.i. implica l'accettazione delle prescrizioni qui contenute.

"fondato sospetto" consente al datore di lavoro di porre la sua azione al di fuori del perimetro di applicazione diretta dell'art. 4 St. lav. e tenuto altresì conto del più generale criterio legale L. n. 604 del 1966, ex art. 5 che grava la parte datoriale dell'onere di provare il complesso degli elementi che giustificano il licenziamento" (…) "allegazione e prova che devono riguardare anche circostanze temporalmente collocate, atteso che le stesse segnano il momento a partire dal quale i dati acquisiti possono essere utilizzati nel procedimento disciplinare e, successivamente, in giudizio, non essendo possibile l'esame e l'analisi di informazioni precedentemente assunte in violazione delle prescrizioni di cui all'art. 4 St. lav., estendendo "a dismisura" l'area del controllo difensivo lecito (cfr. Cass. n. 25732/2021 cit., punto 41), considerato che non può essere reso retroattivamente lecito un comportamento che tale non era al momento in cui fu tenuto" (Cass. Civ. sez. lav. - 26/06/2023, n. 18168).

In caso di cambi di mansione o di interruzione del rapporto di lavoro, si procede all'immediata revoca delle credenziali.

I profili sono soggetti a revisione periodica.

Nel caso in cui si affidino a fornitori esterni attività di manutenzione o di supporto nell'uso dei sistemi informatici o di elaborazione o trattamento, per conto della società, di dati o informazioni, pertinenti ai s.i. della società, ovvero si affidino attività che implichino o possano implicare accesso ad archivi, a registri, a libri della società, o dati o informazioni personali, sensibili o riservati per loro natura o a seguito di impegni assunti dalla Società, questi fornitori sono vincolati al rispetto di obblighi di riservatezza.

Chi svolge l'attività di manutenzione che venga a conoscenza di attività illecite operate sul s.i. in manutenzione è tenuto a informarne l'A.U. della Società.

La violazione di tali obblighi comporta la sanzione previste dal codice disciplinare.