NOVE S.p.A.

Modello Organizzativo ex d. lgs. 231/2001

PARTE GENERALE

Allegato 4.5

Protocollo Sistemi informatici

Revisione	Approvazione	Natura della modifica
Rev.0	12/09/2012	Adozione
Rev.1	CDA del 17/03/2020	Aggiornamento complessivo

Sommario

1. SCOPO

Scopo del presente protocollo 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 e dei fenomeni corruttivi;

b) Garantire la sicurezza dei sistemi informatici della società.

Il presente protocollo costituisce altresì regolamento per l'uso della posta elettronica e di internet, a mente del provvedimento del Garante per la tutela dei dati personali (di seguito anche "Garante") dellì 10/3/2007 e s.m.i.

2. AMBITO

Il presente protocollo ha ad oggetto l'utilizzo dei sistemi informatici della Società e si rivolge a tutti gli Utenti e Amministratori di Sistema.

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 rete informatica aziendale o a dati, informazioni o programmi pertinenti alla Società.

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.

Per "amministratore di sistema" si intende il soggetto al quale è conferito il compito di sovrintendere alle risorse dei sistemi informatici della Società.

3. PRINCIPI GENERALI

Lo svolgimento dell'attività in oggetto deve improntarsi al rispetto delle vigenti disposizioni di legge, nonché dei principi e delle misure di prevenzione dei reati e dei fenomeni corruttivi.

Al fine di assicurare correttezza e trasparenza, è operata la segregazione delle funzioni lungo tutte le fasi del processo, onde consentire una serie di controlli a catena e l'imputazione delle responsabilità per le scelte

compiute. Tutte le operazioni relative all'oggetto della presente sono compiute da soggetti identificabili e sotto la supervisione del superiore gerarchico.

Le presenti misure si applicano anche quando gli utenti usino sistemi informatici di soggetti terzi. I soggetti terzi che forniscano sistemi informatici sono vincolati al rispetto delle misure di prevenzione previste dal Modello.

La società si dota delle misure di tutela dei dati personali a norma delle disposizioni vigenti a tutela dei dati personali. Il presente protocollo si applica in quanto non sia incompatibile con tali disposizioni.

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 dall'amministratore di sistema, in accordo con le disposizioni dell'A.D., sentito il responsabile di funzione.

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.D., all'amministratore di sistema e all'O.d.V. e al R.P.C. 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.

Può essere data in uso agli utenti una casella di posta elettronica con account personale. L'uso di posta elettronica attraverso questa casella 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 utenze, 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.

Nei limiti della normativa vigente a tutela dei dati personali, l'amministratore di sistema, l'A.D., ovvero dipendenti Iren con atto dell'A.D., sono autorizzati ad accedere ai sistemi informatici e a prendere cognizione dei dati, programmi, informazioni, messaggi di posta elettronica ad essi pertinenti, ai fini di garanzia della continuità dell'attività d'impresa, di manutenzione e di tutela della sicurezza dei sistemi medesimi (operazioni di tutela).

Sempre nei limiti delle normative vigenti, il responsabile di commessa, l'A.D. e/o l'amministratore di sistema compie verifiche periodiche direttamente sui s.i. in ordine al loro corretto impiego, al rispetto delle prescrizioni contenute nel presente protocollo ed ai fini di prevenzione dei reati per i quali trova applicazione il d. lgs. 231/2001 (operazioni di controllo). Le operazioni di controllo sono effettuate preferibilmente alla presenza dell'utente.

Tutta la corrispondenza con l'O.d.V. e con il R.P.C. 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 o sensibili ai sensi delle norme vigenti, 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.D.

Il presente protocollo è comunicato a tutti gli utenti.

4. PRINCIPI DI CONDOTTA

Le assegnazioni in uso di un sistema informatico o telematico o di un profilo dipendono dalle mansioni assegnate o sono disposte dall'AD. I profili e l'uso dei sistemi informatici sono assegnati unicamente dall'amministratore di sistema. 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.

Con la concessione in uso di un sistema informatico e/o l'assegnazione di un profilo, ovvero la modifica del medesimo, l'utente riceve il presente protocollo e ne sottoscrive copia per accettazione delle prescrizioni in essi contenute ed autorizzazione senza riserve ai soggetti preposti alle operazioni di tutela e di controllo all'accesso ai s.i. assegnati all'utente nonché ai dati alle informazioni, ai programmi, alla posta elettronica in essi contenuti o ad essi pertinenti, nonché alla loro conservazione ed utilizzo, nei limiti qui specificati.

Ad ogni cambio di mansione il responsabile di funzione dell'utente e/o il responsabile di commessa, comunica la necessità del cambio di profilo all'amministratore di sistema, il quale provvede alla revoca immediata del precedente profilo. Per l'autorizzazione ed assegnazione di un nuovo profilo si applicano le prescrizioni precedenti.

Si procede all'immediata revoca di User-Id e profilo, come le modalità sopra descritte, nel caso di interruzione del rapporto con la Società. Si applica il Protocollo "Personale".

I profili sono soggetti a revisione periodica.

La manutenzione di sistemi informatici (sw ed hw) è responsabilità dell'amministratore di sistema, il quale supervisione altresì l'opera di eventuali fornitori esterni. Il manutentore è vincolato – se esterno alla società, con apposito contratto – alla riservatezza sui dati, informazioni, programmi inerenti ai s.i. in manutenzione, nonché al rispetto dei principi del Modello. La violazione di tali obblighi comporta la sanzione previste dal codice disciplinare.

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 e dei principi previsti dal modello di organizzazione, gestione e controllo della società.

Chi svolge l'attività di manutenzione che venga a conoscenza di attività illecite operate sul s.i. in manutenzione è tenuto a informarne l'Organo Amministrativo della Società, l'O.d.V. ed il R.P.C.

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

5. NORME RELATIVE ALL'AMMINISTRATORE DI SISTEMA

L'amministratore di sistema è nominato dall'A.D.

La nomina deve ricadere su persona dotata dei requisiti previsti dalle disposizioni del Garante (capacità ed affidabilità nel rispetto delle norme vigenti).

La nomina è fatta con atto scritto indicante puntualmente le attività a questo assegnate, alla luce del presente protocollo e delle ulteriori esigenze operative della società. La nomina scritta è conservata dall'amministrazione e messa a disposizione del Garante, a richieste di questo. Il suo nominativo è comunicato all'O.d.V., al R.P.C. e a tutti gli utenti.

L'amministratore di sistema opera, con password nominative nelle funzioni di a) utente; b) amministratore di rete; c) amministratore del s.i.

L'attività dell'amministratore di sistema è tracciata mediante la registrazione dei file di log, a norma del provvedimento del Garante 27/11/2008 s.m.i. I file di log sono registrati e conservati per un massimo di 12 mesi, con modalità tali da assicurarne completezza, inalterabilità e verifica della loro integrità. Le registrazioni devono comprendere i riferimenti temporanei, la descrizione dell'evento e l'identificazione dell'amministratore di sistema.

L'amministratore di sistema riferisce periodicamente all'A.D., all'O.d.V. e al R.P.C. delle operazioni di tutela e di controllo svolte e dei loro esiti.

6. ITER OPERATIVO

A- CREAZIONE di NUOVO PROFILO.

L'utente trasmette all'amministratore di sistema la richiesta di creazione di un'utenza informatica, indicando, con il maggior grado di dettaglio possibile, le mansioni nonché delle necessità di uso dei s.i.

L'amministratore di sistema trasmette quindi richiesta di autorizzazione all'attivazione all'A.D., il quale verificata la coerenza con il mansionario per il quali l'utente è stato assunto ed i precedenti disciplinari, autorizza l'assegnazione. Con l'autorizzazione può disporre il ricorso a filtri e/o blocchi specifici.

Ottenuta l'autorizzazione, l'amministratore di sistema attiva il profilo, assegnando un User-id (immodificabile) e le password necessarie. Attiva altresì contestualmente i blocchi ed i filtri per l'utente. Inserisce l'utente nell'archivio utenze, con il nominativo dell'utente, la User-id, le password, il tipo, la collocazione ed il numero seriale dei sistemi informatici lasciati in uso, il loro indirizzo IP, le mansioni, il profilo assegnato.

L'amministratore di sistema predispone inoltre la modulistica per l'attivazione, il presente protocollo, una dichiarazione attestante la ricezione, l'accettazione delle prescrizioni contenute, nonché le autorizzazioni agli accessi e al trattamento dei dati, il tipo e le caratteristiche. L'utenza rimane bloccata fino a che non è ricevuta la sottoscrizione dell'utente.

L'utente, sottoscritte il presente protocollo e le autorizzazioni richieste, prende possesso del s.i., dell'User Id e delle password. Le password sono consegnate in busta chiusa all'amministrazione e all'amministratore di sistema.

B – MODIFICHE AL PROFILO

Quando richiesto dal cambio delle mansioni assegnate, ovvero delle esigenze di servizio, si procede alla modifica di profilo.

Si applicano le disposizioni previste per l'assegnazione di un nuovo profilo, con cambio dell'User-ID. Le richieste di assegnazione del nuovo profilo spettano al responsabile della funzione di assegnazione o di commessa.

Il cambio del profilo può avvenire anche per motivi disciplinari. Si applica il codice disciplinare.

C - REVOCA DEL PROFILO

Se la revoca avviene per motivi disciplinari, si applica il codice disciplinare.

Quando si interrompono i rapporti con la società, l'A.D. informa con immediatezza l'amministratore di sistema del giorno il cui l'utente non necessita più del profilo. Il profilo è revocato dall'amministratore di sistema il giorno stesso, e la User ID cancellata dal sistema, con la revoca di ogni autorizzazione e facoltà ad essa correlata.

D – CAMBIO DI POSTAZIONE, che non comporti mutamenti nel profilo

E' richiesto o autorizzato dal responsabile di commessa o di funzione, sentito se del caso il RSPP. L'amministratore di sistema effettua le verifiche tecniche del caso, sotto la supervisione del RSPP anche in funzione delle prescrizioni del d. lgs. 81/2008.

L'amministratore di sistema aggiorna l'archivio utenze.

E – RESTITUZIONE del s.i. assegnato

Il s.i. assegnato deve essere restituito, quando si interrompe il rapporto con la società.

In questo caso, si procede all'immediata cancellazione di tutti i dati contenuti nelle memorie del s.i., con la sola eccezione dei casi per i quali il rapporto è stato interrotto in relazione all'uso del s.i. In tal caso si conservano i dati pertinenti ad un reato, ovvero ad un illecito ai sensi del codice disciplinare della società, nei limiti di tempo e le modalità consentite dalla legge.

Può procedersi al cambio di s.i. assegnato con il cambio di mansione o di postazione, nonché per motivi di manutenzione. In ogni caso, si procede a disabilitare le password di accesso al s.i. I manutentori accederanno con loro password, assegnata allo scopo. Conclusa la manutenzione e restituito il s.i., si assegnerà nuova password di accesso provvisoria.

Se il s.i. è destinato a nuovo utente, operata la rimozione e restituzione dei dati e delle informazioni di esclusiva pertinenza del precedente utente, la funzione s.i. procede alla formattazione del s.i. ed a rendere questa disponibile per nuova utenza.

E' cura dell'amministratore di sistema l'aggiornamento costante dell'archivio User-ID.

7. SANZIONI

Le violazioni delle disposizioni qui contenute sono sanzionati in base al sistema disciplinare adottato dalla società ai sensi del d. lgs. 231/2001 e L. 300/1970.

8. NORME DI RIFERIMENTO

D. Lgs. 231/2001, GDPR, (adottato dall´Autorità il 1° marzo 2007 e pubblicato in Gazzetta Ufficiale n. 58 del 10 marzo 2007), L. 300/1970, D. Lgs. 81/2008, Codice di condotta della società e loro successive modificazioni ed integrazioni.