2021

REGOLAMENTO SULLE MODALITÀ D'USO

DEGLI STRUMENTI INFORMATICI,

DI INTERNET E DELLA POSTA ELETTRONICA

Via Vida, 10 – 12051 ALBA (CN)
Tel +39 0173.316111 Fax +39 0173.316480
e-mail: aslcn2@legalmail.it – www.aslcn2.it

P.I./Cod. Fisc. 02419170044

SOMMARIO

Via Vida, 10 – 12051 ALBA (CN)
Tel +39 0173.316111 Fax +39 0173.316480
e-mail: aslcn2@legalmail.it – www.aslcn2.it

P.I./Cod. Fisc. 02419170044

1. OGGETTO

Il presente regolamento disciplina:

- le modalità di utilizzo degli strumenti informatici nell'ambito dello svolgimento delle proprie mansioni, dei propri compiti di lavoro e nelle attività di ufficio da parte di coloro che hanno in dotazione una stazione di lavoro di tipo personal computer e dispositivi mobile e le relative responsabilità;
- le modalità di utilizzo di strumenti di comunicazione informatica come Internet e Posta Elettronica e le relative responsabilità;
- i controlli predisposti dall'Azienda al fine di verificare il corretto utilizzo, la funzionalità e la sicurezza delle risorse informatiche.

2. DEFINIZIONI

OGGETTO	DEFINIZIONI
IT	S.C. Informatica, Telecomunicazioni e Sistema Informativo
PDL	Postazione di Lavoro, normalmente costituita da un Personal Computer (acquistata o a noleggio, messa a disposizione dall'A.S.L. CN2 e gestita dall'IT) e da una stampante, sia individuale che di rete

3. AMBITO DI APPLICAZIONE

Il presente regolamento si applica alle seguenti tipologie di utenti:

- personale dipendente;
- personale convenzionato;
- personale esterno a vario titolo (lavoratori interinali, co.co.pro., consulenti a P. IVA, ecc.);
- altri casi specificamente autorizzati dalla Direzione.

Gli ultimi due casi sono realizzabili esclusivamente dopo aver individuato tale personale come responsabile esterno o personale dipendente autorizzato da responsabile esterno o come personale autorizzato interno (incaricato del trattamento secondo la dizione del Codice privacy)

Le suddette tipologie utenti si classificano in due categorie, a seconda della PDL utilizzata:

- **PDL aziendale**, che può essere utilizzata da tutte le tipologie di utenti;
- **PDL non aziendale**, solitamente utilizzata da personale esterno (medici, consulenti, tecnici di ditte fornitrici, ecc.) e di proprietà dello stesso o della ditta di appartenenza.

Le regole seguenti valgono per tutte le tipologie di utenti e di postazioni elencate, salvo dove diversamente specificato.

Via Vida, 10 – 12051 ALBA (CN)
Tel +39 0173.316111 Fax +39 0173.316480
e-mail: aslcn2@legalmail.it – www.aslcn2.it

P.I./Cod. Fisc. 02419170044

4. UTILIZZO DEGLI STRUMENTI INFORMATICI

4.1 PREMESSA

La PDL affidata all'utente è uno strumento di lavoro. Ogni utilizzo non inerente l'attività lavorativa non è consentito in quanto può causare disservizio, costi di manutenzione e pregiudizio alla sicurezza aziendale.

4.2 MODALITA' DI ACCESSO ALLA RETE AZIENDALE

4.2.1 CREDENZIALI DI AUTENTICAZIONE

L'accesso alla rete dati aziendale è protetto mediante l'utilizzo di credenziali di autenticazione.

Le credenziali di autenticazione sono costituite da un codice di identificazione (nome utente), definito dalla S.C. Informatica, Telecomunicazioni e Sistema Informativo (nel seguito "IT"), e da una parola chiave (password) segreta, definita dall'utente.
Il nome utente è diverso per ogni utente e univocamente legato al nominativo dell'utente stesso.
La password deve rispettare alcune elementari regole di sicurezza informatica:

- Regola di lunghezza: la password deve essere composta almeno da otto caratteri;
- Regola di complessità: la password deve essere composta con criteri di complessità, cioè la password deve contenere almeno le seguenti tre categorie di caratteri: minuscoli, maiuscoli, numeri (il sistema rifiuta in automatico l'inserimento di password che non rispettino tali regole); inoltre non deve contenere riferimenti espliciti al nome e cognome dell'utente (il sistema rifiuta in automatico l'inserimento di password che non rispettino tali regole) o altre parole facilmente riconducibili alla sua identità;
- Regola di scadenza: il sistema richiede il cambio della password ogni tre mesi;
- Regola di unicità: durante il cambio della password, il sistema rifiuta l'inserimento delle ultime cinque password inserite;

La parola chiave deve essere mantenuta segreta dall'incaricato, quindi non può essere rivelata ad altri né memorizzata su supporti cartacei o con altre modalità facilmente accessibili.
La parola chiave deve consentire di superare una procedura di autenticazione, relativa a uno specifico trattamento o a un insieme di trattamenti, che consente di identificare l'utente e garantire la sicurezza dei dati inseriti.

Il codice per l'identificazione dell'utente non può essere assegnato ad altri incaricati, neppure in tempi diversi.

Il Responsabile della Struttura o del Dipartimento deve comunicare tempestivamente all'IT ogni variazione relativa all'incarico dell'utente (es. dimissioni, cambio struttura o mansioni), in modo da consentire all'IT di applicare le conseguenti variazioni al profilo autorizzativo informatico dell'utente.

L'IT provvede a disattivare le credenziali di autenticazione non utilizzate da almeno sei mesi.

Via Vida, 10 – 12051 ALBA (CN)
Tel +39 0173.316111 Fax +39 0173.316480
e-mail: aslcn2@legalmail.it – www.aslcn2.it

P.I./Cod. Fisc. 02419170044

Gli utenti non devono mai lasciare incustodito e accessibile il PC durante una sessione di trattamento. Per questo motivo è OBBLIGATORIO utilizzare la funzione "Blocca computer", che richiede l'inserimento delle credenziali per poter riprendere il lavoro, ma senza riavviare il computer.

4.2.2 RICHIESTA CREDENZIALI

Le credenziali di autenticazione devono essere richieste all'IT dal Responsabile della Struttura, Dipartimento o Direzione di appartenenza dell'incaricato. E' ammesso l'uso della e-mail, purchè sia inviata specifica richiesta dal Responsabile oppure, se inviata da altri, venga inviata per conoscenza al Responsabile.

4.3 NORME COMPORTAMENTALI

Durante l'espletamento della propria attività lavorativa:

NON È CONSENTITO:

a) modificare la configurazione hardware e software di funzionamento della postazione di lavoro (nel seguito PDL);
b) installare qualsiasi tipo di software su una PDL, se non autorizzato dall'IT ;
c) installare o duplicare software non coperto da regolare licenza fornita dall'IT;
d) alterare la configurazione di rete assegnata dall'IT alla PDL (anche PDL non aziendali);
e) disattivare, anche temporaneamente, il software ANTIVIRUS installato dall'IT, né installare altri software antivirus;
f) aprire canali informativi telematici non autorizzati, da e verso l'esterno alla Azienda in qualsiasi forma (ad es. collegamento via modem o via chiavette Internet wireless, tramite Internet, ecc.) (anche PDL non aziendali);
g) utilizzare programmi non attinenti alla propria attività lavorativa, anche se regolarmente acquistati o facenti parte della dotazione della PDL;
h) memorizzare sulla propria postazione di lavoro, o su archivi rimovibili utilizzabili sulla stessa PDL, archivi informatici contenenti archivi personali che non rispondono alla normativa vigente.
i) memorizzare su di una PDL file o archivi informatici non afferenti l'attività lavorativa (es. musica, film, programmi, se non utilizzati per motivi di lavoro).
j) Memorizzare dati aziendali su piattaforme in cloud non autorizzate dall'Azienda..

È OBBLIGATORIO:

k) segnalare al Responsabile della Struttura di appartenenza le eventuali condizioni anomale che possono pregiudicare il rispetto delle norme di comportamento indicate nel presente regolamento. In particolare, nel caso di PDL utilizzate da più utenti, è richiesto di segnalare al Responsabile della Struttura di appartenenza eventuali installazioni di software non autorizzato.
l) Ogni PDL o dispositivo collegato alla rete aziendale (cablata o wireless) deve essere preventivamente autorizzato dall'IT.

Via Vida, 10 – 12051 ALBA (CN)
Tel +39 0173.316111 Fax +39 0173.316480
e-mail: aslcn2@legalmail.it – www.aslcn2.it

P.I./Cod. Fisc. 02419170044

Per le PDL <u>non aziendali</u>, si aggiungono le seguenti regole:

m) Rispetto delle regole sottoscritte in fase di individuazione come responsabile esterno o come incaricato esterno.
n) la PDL deve essere configurata a cura dell'utente in modo da non arrecare alcun danno, pericolo o intralcio all'attività lavorativa aziendale;
o) la PDL deve utilizzare software aggiornato ed in regola con le vigenti leggi (es. D. Lgs. 196/2003);
p) i software installati sulla PDL e che fanno uso della rete aziendale devono essere autorizzati dall'IT;
q) in particolare la PDL deve disporre di software antivirus **aggiornato sempre attivo** e non devono essere installati software di tipo malevolo o che possano sottrarre dati, anche in modo nascosto;
r) l'A.S.L. CN2, nel caso venga riscontrato un danno causato dall'uso non conforme al presente regolamento di una PDL non aziendale, si riserva di rivalersi nei confronti del proprietario della stessa.

4.4 MANUTENZIONE DELLE POSTAZIONI DI LAVORO

4.4.1 GESTIONE DELLE POSTAZIONI

La consistenza attuale del parco macchine delle postazioni di lavoro è di circa 1200, per cui risulta indispensabile utilizzare strumenti automatici per la loro gestione. In particolare l'IT utilizza un sistema che consente di acquisire e raccogliere automaticamente in un archivio centralizzato le **configurazioni hardware e software di base** di tutte le **<u>PDL aziendali</u>**, in modo da poter conoscere con esattezza in qualsiasi momento le caratteristiche di una macchina o poter pianificare interventi mirati o generalizzati di aggiornamento.

Va sottolineato che il suddetto sistema si limita ad acquisire la configurazione, mentre **non rileva l'attività in corso**, quindi non è in nessun caso identificabile come uno strumento per controllare l'attività lavorativa.

4.4.2 MODALITA' DI EFFETTUAZIONE DEGLI INTERVENTI DI MANUTENZIONE

In <u>caso di malfunzionamento</u> di una PDL aziendale, il personale tecnico dell'IT potrà effettuare i seguenti interventi:

a) attivare un collegamento da remoto, mediante appositi programmi presenti sulla postazione, per verificare il problema e, possibilmente, risolverlo. In questo caso il tecnico IT dovrà preventivamente contattare (telefonicamente) l'utente della postazione per avvisarlo dell'operazione. Nel caso in cui l'utente non sia contattabile, il tecnico IT potrà decidere, in base a criteri di efficienza ed economia aziendale dettati dalla natura della richiesta (es. urgenza), se effettuare comunque il collegamento oppure attendere la disponibilità dell'utente;
b) concordare con l'utente o, in sua assenza, con il responsabile o altro personale della struttura di appartenenza, un intervento in loco.

Via Vida, 10 – 12051 ALBA (CN)
Tel +39 0173.316111 Fax +39 0173.316480
e-mail: aslcn2@legalmail.it – www.aslcn2.it

P.I./Cod. Fisc. 02419170044

Per le PDL non aziendali, non è prevista manutenzione da parte dell'A.S.L. CN2.

5. ACCESSO AD INTERNET

Per quanto riguarda l'accesso alla rete Internet e relativi siti, quanto di seguito riportato si applica al personale dipendente e al personale non dipendente che sia stato preventivamente autorizzato per l'accesso:

a) la navigazione in Internet è consentita da tutte le PDL, tranne quelle dedicate ad attività specifiche
b) data la vasta gamma di attività aziendali, non è stato definito a priori un elenco di siti aziendali autorizzati; è stato invece attivato un apposito software di filtraggio, comune a tutti gli utenti, mediante il quale risulta bloccata la navigazione su siti i cui contenuti sono stati classificati come estranei agli interessi ed alle attività aziendali;
c) il divieto di accesso ad un sito appartenente alle categorie inibite viene visualizzato esplicitamente a video;
d) non è consentito scaricare da Internet (download) file musicali, video o software che non siano necessari alla propria attività aziendale ed autorizzati dall'IT o dal proprio responsabile di struttura complessa, dipartimento o direzione;
e) non è consentito l'accesso a social network (es. Facebook, Twitter, ecc.), chat esterne (es. Messenger), giochi on line, ed ad altre applicazioni on-line non finalizzate all'attività lavorativa.

6. USO DELLA POSTA ELETTRONICA

La posta elettronica (e-mail) aziendale costituisce il principale strumento aziendale per le comunicazioni interne. La casella di posta elettronica va intesa come mezzo di comunicazione e non come luogo di archiviazione dei file: tutti i messaggi e gli allegati che si vogliono conservare devono essere salvati sulle cartelle di rete del proprio servizio.
Esistono due tipologie di caselle postali aziendali, tutte abilitate sia all'interno dell'azienda che all'esterno:

- Casella nominativa individuale;
- Casella del servizio ed istituzionali.

6.1 REGOLE PER LA CASELLA INDIVIDUALE

La casella di posta elettronica è uno strumento di lavoro e come tale deve essere utilizzata esclusivamente ai fini dello svolgimento dell'attività lavorativa.
La posta elettronica è concessa a tutti i dipendenti autorizzati ad utilizzare una PDL aziendale e dotati di credenziali individuali rilasciate dall'IT. Di norma non è prevista la concessione di caselle di posta aziendali ad utenti che utilizzano PDL non aziendali, salvo esplicita autorizzazione della Direzione.
Le regole comportamentali relative all'utilizzo di una casella personale di posta elettronica sono le seguenti:

Via Vida, 10 – 12051 ALBA (CN)
Tel +39 0173.316111 Fax +39 0173.316480
e-mail: aslcn2@legalmail.it – www.aslcn2.it

P.I./Cod. Fisc. 02419170044

a) ogni utente è responsabile dell'impiego effettuato della propria casella postale;
b) l'accesso alla casella è strettamente personale e non può essere delegato ad altri;
c) quanto riportato nei messaggi impegna sia il mittente che l'azienda sui loro contenuti nei confronti dei destinatari. L'azienda si riserva di rivalersi sul lavoratore nel caso l'utilizzo della casella postale elettronica, come di qualsiasi altro mezzo di comunicazione, violi le leggi vigenti o sia contrario alle direttive ed agli interessi dell'azienda;
d) non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, *Forum, newsletter* o *mail-list,* non attinenti l'attività lavorativa;
e) ogni casella ha una dimensione massima, raggiunta la quale ne viene bloccato l'utilizzo. Sarà responsabilità dell'utente segnalare all'IT l'approssimarsi del limite e concordare con lo stesso le opportune misure;
f) esiste un limite sulla dimensione dei messaggi sia in arrivo che in partenza. I messaggi che superano il limite non vengono accettati dal sistema di posta;
g) ogni utilizzatore della casella postale deve gestire propriamente tutti i messaggi ricevuti, ovvero:
    1) inviare il messaggio alla protocollazione quando necessario;
    2) inoltrare ai colleghi o ad altri servizi interessati documenti di loro competenza;
    3) impostare le regole di fuori sede per avvisare i mittenti in caso di assenze superiori ai 5 giorni;
    4) cancellare le mail vecchie e non più utili;
    5) salvare messaggi ed allegati sulle cartelle di rete;
    6) evitare di aprire messaggi di posta provenienti da mittenti sconosciuti;
    7) evitare di aprire allegati di cui non si conosce il contenuto;

6.2 REGOLE DI BASE CASELLE DI SERVIZIO ED ISTITUZIONALI

La posta elettronica di servizio non deve essere una casella con password condivisa. Può essere una casella di posta a cui ciascuno del servizio, opportunamente e formalmente autorizzato dal Responsabile di Servizio entra con propria password e quindi rimane collegata alla propria casella di posta.
Nelle istruzioni impartite per l'utilizzo della posta elettronica deve essere richiesto obbligatoriamente che chi scrive un messaggio con la posta elettronica di servizio si firmi in modo da evidenziare, eventualmente anche all'esterno dell'Azienda, chi è che ha letto e quindi risponde ad una mail.
Per creare una casella postale relativa ad un servizio, il responsabile di struttura complessa, dipartimento o direzione a cui appartiene il servizio deve farne richiesta all'IT, indicando l'elenco dei dipendenti che dovranno essere abilitati ad accedere alla casella.

Via Vida, 10 – 12051 ALBA (CN)
Tel +39 0173.316111 Fax +39 0173.316480
e-mail: aslcn2@legalmail.it – www.aslcn2.it

P.I./Cod. Fisc. 02419170044

6.3 REGOLE COMUNI

Nei messaggi inviati tramite caselle e-mail aziendali (di servizio e/o nominative) verso l'esterno, deve essere accluso il seguente testo: "*Si segnala che il presente messaggio e le risposte allo stesso potranno essere conosciute dall'organizzazione lavorativa di appartenenza del mittente secondo le modalità previste dal regolamento Aziendale adottato in materia. Se per un disguido avete ricevuto questa e-mail senza esserne i destinatari vogliate cortesemente distruggerla e darne informazione all'indirizzo mittente*".

Nel caso in cui per assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, l'interessato deve delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare-responsabile del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Il nominativo del fiduciario deve essere comunicato al Responsabile della Struttura o Dipartimento di appartenenza.
In mancanza della nomina di un fiduciario, su richiesta del suddetto Responsabile, gli Amministratori di Sistema potranno accedere alla posta elettronica del lavoratore assente. L'IT dovrà fare in modo che l'utente debba modificare la propria parola chiave al primo accesso successivo e dovrà provvedere ad informare l'utente di quanto avvenuto.

Il contenuto dei messaggi di posta elettronica e gli eventuali allegati indirizzati ad utenti esterni all'Azienda non possono contenere dati particolari in chiaro. Pertanto, nei limitati casi in cui sia istituzionalmente indispensabile gestirne l'invio, è obbligatorio predisporre un allegato che deve essere criptato con password. Tale chiave di accesso deve essere comunicata al destinatario con un mezzo diverso dal sistema di posta aziendale.

6.3.1 Accesso in mobilità

Il sistema di posta elettronica aziendale è in fase di sostituzione, pertanto le policy di utilizzo in mobilità verranno ridefinite una volta completata la messa in funzione.

6.4 MODALITA' DI ASSEGNAZIONE DELLE CASELLE DI POSTA ELETTRONICA AL PERSONALE NON DIPENDENTE

Per quanto attiene il personale non dipendente che collabora a vario titolo con l'Azienda, le caselle di posta elettronica sono assegnate con le seguenti modalità:

TIPOLOGIA DI PERSONALE	MODALITA' DI ASSEGNAZIONE DELLE CASELLE DI POSTA ELETTRONICA
Medici di Continuità Assistenziale (Guardia Medica)	Si
Dipendenti Società in-house (es. AMOS)	Si

Via Vida, 10 – 12051 ALBA (CN)
Tel +39 0173.316111 Fax +39 0173.316480
e-mail: aslcn2@legalmail.it – www.aslcn2.it

P.I./Cod. Fisc. 02419170044

Salvo quanto previsto al periodo precedente, ai soggetti di cui al presente paragrafo si applicano le regole previste per il personale dipendente.

7. CONTROLLI

L'IT dispone di appositi strumenti che registrano i dati di utilizzo dei sistemi.
Tali dati sono:

1. Accessi degli utenti alla rete, contenenti: codice utente, data e ora evento, operazione ingresso/uscita (login/logout).
2. Accessi degli utenti ad internet, contenenti: indirizzo IP postazione origine, indirizzo IP sito Internet destinatario, data e ora evento. L'indirizzo IP consente di stabilire univocamente, se necessario, qual è la postazione aziendale o il server del sito interessati, al netto della riassegnazione dinamica dell'indirizzo.
3. Accessi degli utenti agli applicativi, dove disponibili, contenenti: codice utente, data e ora evento, tipo di operazione.

Qualora le misure tecniche preventive non fossero sufficienti ad evitare eventi dannosi o situazioni di pericolo, l'Azienda effettua con gradualità, nel rispetto dei principi di pertinenza e non eccedenza, le verifiche di eventuali situazioni anomale attraverso le seguenti fasi:

• analisi aggregata del traffico di rete riferito all'intera struttura lavorativa o a sue aree (reparto, servizio, ecc.) e rilevazione della tipologia di utilizzo (e-mail, file audio, accesso a risorse estranee alle mansioni);
• emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo degli strumenti aziendali, con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite; il richiamo all'osservanza delle regole può essere circoscritto agli operatori afferenti al settore in cui è stata rilevata l'anomalia;
• in caso di successivo permanere di una situazione non conforme, é possibile effettuare controlli circoscritti su singole postazioni di lavoro.

Con la stessa gradualità vengono effettuati controlli sull'occupazione dello spazio di memorizzazione sui server aziendali attraverso le seguenti fasi:

• analisi aggregata dei dati memorizzati sui server a livello di intera struttura lavorativa (reparto, servizio, ecc.) e rilevazione della tipologia di utilizzo (file audio, file video, immagini, software non autorizzato) e relativa pertinenza con l'attività lavorativa;
• emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo degli strumenti aziendali, con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite; il richiamo all'osservanza delle regole può essere circoscritto agli operatori afferenti il settore in cui è stata rilevata l'anomalia;
• in caso di successivo permanere di una situazione non conforme, è possibile procedere con un analisi puntuale ed una eventuale eliminazione del materiale non conforme anche sulle singole postazioni di lavoro.

Via Vida, 10 – 12051 ALBA (CN)
Tel +39 0173.316111 Fax +39 0173.316480
e-mail: aslcn2@legalmail.it – www.aslcn2.it

P.I./Cod. Fisc. 02419170044

I dati necessari alla generazione dei report vengono conservati per la durata massima di 30 gg., salvo diverse disposizioni di legge o l'ipotesi in cui, a seguito dei controlli di cui sopra, emergano fatti aventi rilevanza penale e/o disciplinare e contabile o che comportino responsabilità erariale, nel qual caso verranno conservati fino alla conclusione dei suddetti procedimenti. Il tempo di conservazione è in ogni caso determinato in funzione dei limiti tecnici dei sistemi in dotazione.
I controlli di cui sopra verranno effettuati sui dati registrati dalla data di entrata in vigore del Regolamento.
Per quanto riguarda gli Amministratori di Sistema il controllo di cui sopra viene effettuato dal Responsabile della S.C. Informatica, Telecomunicazioni e Sistema Informativo.

8. AMMINISTRATORI DI SISTEMA – TECNICI IT

Tutte le informazioni, ivi incluse quelle inerenti dati idonei a rivelare lo stato di salute, cui possono avere accesso, anche occasionalmente, i Tecnici dell'IT nell'esercizio della loro attività di gestione hardware e software o di Amministratori di Sistema (AdS), non possono essere comunicate ad alcuno e non possono essere memorizzate su supporti diversi da quelli d'origine e di backup.
Gli Amministratori di Sistema interni ed i Tecnici dell'IT sono tenuti al segreto d'ufficio.
Per quanto riguarda i sistemi di comunicazione e messaggistica (posta elettronica,…) è fatto divieto anche agli AdS di accedere ai contenuti dei messaggi di terzi, fatto salvo il caso di interventi di assistenza richiesti dagli utenti per i quali gli AdS accederanno tramite assistenza remota sul posto di lavoro previa autorizzazione dell'utente stesso. Il responsabile del S. Informatica e Telecomunicazioni dovrà sfruttare le funzionalità degli applicativi di comunicazione e messaggistica per limitare e/o precludere l'accesso ai contenuti dei messaggi di terzi da parte degli AdS.
Agli Amministratori di Sistema esterni ed alle Ditte che effettuano attività di manutenzione di hardware e software sono state impartite specifiche istruzioni al fine di garantire la riservatezza dei dati, anche personali, dagli stessi acquisiti.

8.1 SISTEMA DI ACCESS LOG

Fermo restando le tipologie di controllo previste dall'art. 7 che trovano applicazione anche nei confronti degli Amministratori di Sistema, ai sensi del provvedimento del 27 novembre 2008 del Garante della Privacy, l'Azienda ha l'obbligo di tenere traccia degli accessi logici degli amministratori di sistema ai sistemi da essi amministrati. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo di tempo, non inferiore a sei mesi.
A tale scopo è predisposto un sistema centralizzato di raccolta dei log dei sistemi che garantisce le caratteristiche di completezza e inalterabilità richieste. Il sistema centralizzato di gestione dei log (log management) raccoglie i log di tutti gli accessi logici degli amministratori di sistemi gestiti sui server aziendali.

Via Vida, 10 – 12051 ALBA (CN)
Tel +39 0173.316111 Fax +39 0173.316480
e-mail: aslcn2@legalmail.it – www.aslcn2.it

P.I./Cod. Fisc. 02419170044

Dettagliati report sugli accessi ai sistemi permettono di ottemperare agli obblighi delle normative.
Le registrazioni comprendono i riferimenti temporali, la descrizione dell'evento che le ha generate e vengono conservate in forma crittografata per un periodo minimo di sei mesi, massimo un anno, salvo casi specifici riferiti a eventuali procedimenti legali in corso.
In particolare sono registrate nei log le seguenti informazioni:

- Sistema amministrato
- Nome utente dell'amministratore
- ora e data di accesso (login)
- ora e data di termine accesso (logout)
- tentativi falliti

Possono essere altresì monitorati gli accessi ai seguenti sottosistemi ritenuti particolarmente critici in azienda:

- sistemi di comunicazione e messaggistica (email);

Tali log sono raccolti e conservati in funzione delle capacità elaborative e di memorizzazione disponibili sui server e sul sistema di Access Log e comunque non oltre un anno, salvo casi specifici riferiti a eventuali procedimenti legali in corso.
Tecnicamente la gestione dei log degli amministratori di sistema è realizzata tramite un software di tipo 'agentless' che raccoglie informazioni da:

- server Windows,
- server Linux,
- database server Oracle
- database server SQL Server
- apparati di rete (firewall, proxy,...)

La gestione del sistema di Access Log è in capo alla S.O.C. Informatica, Telecomunicazioni e Sistema Informativo e deve essere garantita secondo le linee guida del garante della privacy e delle misure definite da AGID.

8.2 VERIFICA DELLE ATTIVITÀ DEGLI AMMINISTRATORI DI SISTEMA

Il Garante per la protezione dei dati personali, nel provvedimento del 27 novembre 2008 prevede un "due diligence" in capo al Titolare relativamente agli "accorgimenti e misure, tecniche e organizzative, volti ad agevolare l'esercizio dei doveri di controllo da parte del titolare" sulle mansioni svolte dagli amministratori di sistema designati.
Con "due diligence" si intende il processo di accertamento che viene messo in atto per verificare la compliance normativa, ovvero il rispetto di specifiche disposizioni impartite dal legislatore, da autorità di settore, da organismi di certificazione e da policy interne.
Il Responsabile della S.O.C. Informatica, Telecomunicazioni e Sistema Informativo, effettua verifiche periodiche con cadenza annuale o su richiesta della Direzione Generale, in presenza di criticità o anomalie, volte a monitorare la conformità dei comportamenti degli amministratori di sistema alle prescrizioni di legge e alle regole stabilite dall'Ente. In particolare estrae dal

Via Vida, 10 – 12051 ALBA (CN)
Tel +39 0173.316111 Fax +39 0173.316480
e-mail: aslcn2@legalmail.it – www.aslcn2.it

P.I./Cod. Fisc. 02419170044

sistema centralizzato di raccolta dei log specifici report che contengono informazioni sugli accessi, sulla loro frequenza e sulla loro distribuzione per fascia oraria giornaliera.
In adempimento alle prescrizioni di legge, tali report sono conservati agli atti del Responsabile della S.C. Informatica, Telecomunicazioni e Sistema Informativo.
.

9. DISPOSIZIONI FINALI

9.1 RESPONSABILITA' DELL'UTENTE

Gli utenti sono responsabili di tutte le operazioni effettuate con il loro identificativo.
In particolare e senza pretesa di esaustività, essi rispondono personalmente dell'invio di messaggi spediti dalla propria casella di posta elettronica e di tutte le attività intraprese con il loro nome utente e con l'indirizzo di rete (IP) della loro PDL.
Gli utenti sono altresì responsabili di eventuali danni materiali arrecati alla PDL per incuria o dolo, nel qual caso l'Amministrazione si riserva di addebitare loro i costi di ripristino.

Nello svolgimento delle attività di trattamento, qualora nasca un dubbio in merito alla liceità dell'operazione di trattamento che ci si accinge a compiere, è necessario richiedere, preventivamente, chiarimenti in merito al Responsabile del trattamento dati personali o al Data Protection Officer aziendale. E' comunque necessario comunicare sempre al Responsabile del trattamento dati personali la necessità di eseguire nuovi trattamenti, indipendentemente dallo strumento che si intende utilizzare. La produzione di documenti cartacei deve essere commisurata alla necessità derivante dalla finalità del trattamento e qualsiasi documento deve essere, se ritenuto necessario, archiviato in posto sicuro o distrutto in modo irrecuperabile.

9.2 COMPITO DI SORVEGLIANZA

I responsabili di ciascuna Struttura hanno il compito di vigilare sul corretto rispetto delle modalità di utilizzo degli strumenti informatici in dotazione ai loro collaboratori, nonché di emanare eventuali ulteriori direttive giudicate necessarie nell'ambito di particolari specificità o responsabilità.

9.3 SANZIONI

L'inosservanza delle presenti disposizioni potrà comportare conseguenze sul piano civile, penale e disciplinare. Le sanzioni disciplinari verranno contestate nel rispetto delle procedure previste dalle disposizioni legislative vigenti nonché dai Contratti Collettivi di categoria e dai Regolamenti e Codici di Comportamento aziendali emanati in materia, nei confronti delle altre tipologie di utenti, con i provvedimenti previsti dai rapporti contrattuali con essi in vigore e dalla vigente legislazione civile e penale

9.4 DISPOSIZIONI DI RINVIO

Per quanto non espressamente previsto e disciplinato dal presente regolamento si rinvia alle disposizioni di legge, di regolamento e contrattuali vigenti nella presente materia, nonché alle

Via Vida, 10 – 12051 ALBA (CN)
Tel +39 0173.316111 Fax +39 0173.316480
e-mail: aslcn2@legalmail.it – www.aslcn2.it

P.I./Cod. Fisc. 02419170044

disposizioni previste da AGID con Circolare 18 aprile 2017, n. 2/2017, recante «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)», pubblicata in Gazzetta Ufficiale (Serie Generale n.103 del 5-5-2017)..

9.5 PUBBLICAZIONE

Il presente disciplinare verrà pubblicato sulla rete intranet aziendale e consegnato a tutti i fruitori degli strumenti informatici all'atto dell'instaurazione del rapporto di lavoro.