Palermo Euro Terminal S.r.l.

Banchina Sammuzzo – Porto di Palermo

POLITICA AZIENDALE SULLA SICUREZZA INFORMATICA

Premessa generale

Il presente documento contiene le disposizioni, le misure organizzative e comportamentali che i dipendenti, consulenti e/o professionisti e/o collaboratori a qualsiasi titolo dell'Azienda, sono chiamati ad osservare per contrastare i rischi informatici.

Premesso che l'utilizzo delle risorse informatiche e telematiche messe a disposizione da Palermo Euro Terminal Srl deve sempre ispirarsi al principio della diligenza e correttezza, con la presente **Politica aziendale sulla sicurezza informatica** s'intende contribuire alla massima diffusione della cultura della sicurezza in Azienda, evitando che qualunque condotta possa creare problemi o minacce alla sicurezza dei sistemi informatici e nel trattamento dei dati.

Pubblicazione

Al presente documento- ed ai suoi futuri aggiornamenti – viene data massima diffusione attraverso la sua pubblicazione sul sito internet di Palermo Euro Terminal e sull'intranet aziendale.

1. **Regolamento sulle modalità di utilizzazione della strumentazione informatica messa a disposizione da Palermo Euro Terminal Srl per per lo svolgimento dell'attività lavorativa e sulle relative procedure di controllo.**

Indice

5.1 Principi

5.2 Finalità

5.3 Modalità di effettuazione dei controlli

Premessa

Il presente regolamento definisce le condizioni di utilizzo del Sistema informatico da parte dei dipendenti, consulenti e/o professionisti e/o collaboratori di Palermo Euro Terminal Srl attraverso gli strumenti messi a disposizione dall'Azienda, per il pieno ed efficace svolgimento delle attività legate ai servizi operativi, dell'amministrazione e dei servizi ad esse correlati.

Tale Sistema informatico risponde ad usi ed obiettivi aziendali e l'operatore che lo utilizza deve orientare il suo comportamento al perseguimento di tali scopi. L'utilizzo del sistema è costantemente monitorato, nel rispetto della normativa sulla privacy e delle norme a tutela del lavoratore. Il regolamento prevede altresì un sistema sanzionatorio collegato all'uso improprio delle strumentazioni informatiche.

Tutti i beni che Palermo Euro Terminal Srl mette a disposizione dei propri dipendenti, collaboratori o consulenti per lo svolgimento dell'attività lavorativa devono essere utilizzati da parte di coloro che vi operano, a qualunque livello e con qualsiasi rapporto, in conformità ai principi espressi dal Codice di comportamento dei dipendenti pubblici D.P.R. n.62 del 2013.

1 Principi generali

L'utilizzo degli strumenti informatici forniti ai dipendenti, collaboratori o consulenti aziendali deve avvenire in modo strettamente pertinente all'attività lavorativa, in maniera lecita, appropriata, efficiente e razionale, tenendo sempre presente l'interesse al risparmio delle risorse aziendali.

Deve altresì rispettare i principi etici e di correttezza e i doveri stabiliti dal sopracitato Codice di comportamento, nonché la privacy e la segretezza dei dati trattati secondo le norme vigenti.

Il presente regolamento disciplina le modalità e finalità di utilizzo della strumentazione informatica, nonché le modalità di controllo di tale utilizzo, per garantire, nel rispetto della dignità e riservatezza delle persone in coerenza anche con la normativa vigente in materia di protezione dei dati personali (D.Lgs.n.196/2003-Regolamento Europeo Privacy Ue 2016/679) e con quanto prescritto dal Garante per la protezione dei dati personali con la delibera n.13 del 1/3/2007, la sicurezza dei dati e del sistema informatico aziendale.

2 Destinatari

Sono destinatari del presente Regolamento tutti i collaboratori di Palermo Euro Terminal Srl con rapporto di lavoro subordinato (di qualsiasi tipologia) e coloro che svolgano, a qualsiasi titolo, attività per conto di Palermo Euro Terminal Srl, accedendo al sistema informatico di quest'ultimo.

3 Modalità di utilizzo della strumentazione informatica

I destinatari di cui al punto 2 si impegnano ad utilizzare la strumentazione informatica nel rispetto dei principi di cui al precedente punto 1 e ad osservare le seguenti norme comportamentali:

3.1 Utilizzo di Internet

L'accesso alla rete internet fornita dall'Azienda è consentito principalmente per scopi di lavoro e per l'accesso a dati ed informazioni concernenti l'attività aziendale; per motivi personali l'accesso è consentito soltanto in caso di necessità e comunque non in modo ripetuto o per periodi di tempo prolungati, vietando di:

a. accedere a siti e/o acquisire e/o diffondere contenuti informatici osceni, o lesivi dell'onorabilità individuale o collettiva, o altro materiale potenzialmente offensivo o diffamatorio. In particolare è estremamente vietata la ricezione, la trasmissione o il possesso di immagini pornografiche e/o pedo pornografiche;
b. partecipare ai social network (a titolo semplificativo, ma non esaustivo facebook, myspace, twitter) ai blog, ai forum di discussione;
c. rimanere collegati per periodo di tempo prolungati a siti musicali, anche se contestualmente si continua la propria attività lavorativa, in quanto ciò può appesantire il traffico della rete;
d. scaricare programmi, anche gratuiti, se ciò non è indispensabile allo svolgimento dell'attività lavorativa, segnalandolo preventivamente al proprio responsabile;
e. accedere a servizi con finalità ludiche o a chat line;
f. accedere a siti per la condivisione e lo streaming di contenuti multimediali e simili.

3.2 Utilizzo del PC, portatili, smart phone, tablet

In caso di allontanamento, anche temporaneo, dalla postazione di lavoro, l'utente non deve lasciare il sistema operativo del proprio pc aperto e deve provvedere a proteggere il proprio computer attraverso la sospensione o il blocco della sessione di lavoro.

Al termine dell'orario di servizio, prima di lasciare gli uffici, deve assicurarsi di avere opportunamente spento il proprio PC.

L'utente è responsabile del PC portatile e/o eventuali accessori a lui assegnati (smart -phone, tablet) e deve custodirli con la massima diligenza, sia all'interno degli uffici, sia durante gli spostamenti esterni. Particolare attenzione deve essere prestata nell'utilizzo e nella custodia del PC portatile, smart phone, tablet, al di fuori della rete e degli uffici dell'Azienda, nella connessione a reti esterne e nella rimozione di eventuali file personali memorizzati nei medesimi.

3.3 Utilizzo delle stampanti e dei materiali di consumo

L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, toner, supporti magnetici, supporti digitali, ecc.) è riservato esclusivamente all'attività lavorativa. Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi.

4 Sicurezza e Privacy

Nell'utilizzo delle strumentazioni informatiche occorre adottare le seguenti cautele:

a. mantenere segrete le proprie credenziali di autenticazione (password), sia quelle d'accesso ai vari programmi utilizzati nell'ambito della propria attività lavorativa, attribuite dal responsabile del sistema informatico;
b. non cedere, una volta autenticati nel proprio PC, l'uso della propria postazione a persone non autorizzate, in particolare per l'accesso ad internet ed ai servizi di posta elettronica;
c. adottare, nello svolgimento della propria attività lavorativa, le necessarie cautele per assicurare la sicurezza dei dati trattati e dei dati che possano fornire indicazioni utili ad un eventuale "hacker"(attaccante dei sistemi informativi) dell'Azienda;
d. utilizzare, in caso di trattamento di dati personali, le cartelle di rete o altri supporti di memorizzazione messi a disposizione dell'Azienda al fine di garantire la disponibilità dei dati anche a seguito di errori o eventi accidentali, grazie al sistema centralizzato di backup;
e. prevedere opportune misure che consentano, in caso di assenza dal luogo di lavoro, ad altri utenti autorizzati l'accesso a dati potenzialmente necessari (per es. salvare i dati presenti sul proprio disco rigido in cartelle condivise su file server);
f. non connettere alla rete interna dell'Azienda apparati esterni (come ad es. router..) che possano compromettere il corretto funzionamento della rete aziendale;
g. non utilizzare strumenti di messaggistica istantanea (a titolo esemplificativo, ma non esaustivo Skype, Messenger,whatsapp) per motivi personali;
h. non introdurre o diffondere nella rete aziendale programmi illeciti ovvero che siano contrari a norme imperative di legge, all'ordine pubblico ed al buon costume;
i. non compiere azioni in violazione delle norme a tutela delle opere dell'ingegno e/o del diritto d'autore;
j. utilizzare la posta elettronica messa a disposizione dall'Azienda per lo svolgimento dell'attività lavorativa, esclusivamente per le specifiche finalità della stessa, nel rispetto delle esigenze di funzionalità e sicurezza dei sistemi informatici;
k. avere cura di non aprire allegati di posta in e-mail dal mittente e/o dall'oggetto sospetti per prevenire i rischi causati da software nocivi (per es. virus, worm,spyware, ecc.);
l. limitare al minimo indispensabile la diffusione del proprio indirizzo e-mail istituzionale su siti web pubblici (a titolo esemplificativo, ma non esaustivo forum, mailing list, ecc.);
m. non rimuovere il programma antivirus installato sulla postazione di lavoro;
n. verificare la presenza di eventuali virus prima di utilizzare supporti rimovibili;

o. nel caso in cui il software antivirus rilevi la presenza di un virus sospendere ogni elaborazione in corso senza spegnere il computer e segnalare l'evento al responsabile; non inviare messaggi di posta elettronica contenenti segnalazioni del virus ad altri utenti;
p. utilizzare sulle postazioni di lavoro esclusivamente il software autorizzato e fornito dall'Azienda; eventuali software aggiuntivi, rispetto all'installazione standard, dovranno essere richiesti al proprio responsabile;
q. non lasciare incustoditi i dispositivi mobili aziendali (come ad esempio i cellulari e i tablet aziendali);
r. in caso di incidente di sicurezza (come ad esempio nei casi di accesso non autorizzato o di minacce informatiche al sistema), attenersi scrupolosamente alle indicazioni ricevute dal personale addetto alla sicurezza ed alla gestione della rete e dei sistemi;
s. nell'utilizzo della posta elettronica certificata, le credenziali (user ID e password) per accedere a tale casella di posta devono essere a conoscenza unicamente dei responsabili autorizzati dal Direttore.

Per quanto riguarda i collaboratori addetti al Sistema informatico aziendale, in ragione delle funzioni svolte, ad essi non si applicano i punti 3.1d, 4.p

5 Controlli

L'Amministrazione si riserva di effettuare controlli sul corretto utilizzo degli strumenti informatici e telematici nel rispetto delle normative vigenti e del presente regolamento, nonché nel rispetto dello Statuto dei Lavoratori.

I controlli vengono effettuati dal responsabile della sicurezza con l'ausilio dell'assistenza tecnica, anche dietro segnalazione proveniente dalle strutture regionali competenti o dagli organi di polizia giudiziaria.

5.1 Principi

L'Azienda ritiene che l'attività di prevenzione debba essere prevalente rispetto all'attività di controllo. Si impegna pertanto a potenziare in misura crescente tale attività di prevenzione, in particolare tramite azioni di sensibilizzazione e di diffusione dei principi e delle regole da osservare nell'utilizzo della strumentazione informatica, nell'adozione di specifiche soluzioni tecnologiche e di ogni altra misura ritenuta idonea a tal fine.

I controlli effettuati dall'Azienda rispettano i seguenti principi:

a) necessità: i dati trattati durante l'attività di controllo sono sempre e soltanto quelli strettamente necessari a perseguire le finalità di cui al paragrafo 5.2;
b) proporzionalità: i controlli sono sempre effettuati con modalità tali da garantire, nei singoli casi concreti, la pertinenza e non eccedenza delle informazioni rilevate rispetto alle finalità perseguite e specificate al paragrafo 5.2;

c) imparzialità: i controlli sono effettuati su tutta la strumentazione informatica messa a disposizione dall'amministrazione aziendale e conseguentemente possono coinvolgere tutti i collaboratori della stessa, a qualunque titolo utilizzino tale strumentazione, fatta eccezione per quella eventualmente assegnata alle rappresentanze sindacali unitarie e agli organi istituzionali. In nessun caso sono effettuati controlli mirati e ripetuti nei confronti di soggetti specifici con finalità discriminatorie o persecutorie o volutamente sanzionatorie;
d) trasparenza: in base a tale principio l'amministrazione mette in atto tutte le azioni necessarie a garantire la preventiva conoscenza da parte di tutti i soggetti potenzialmente sottoposti ai controlli del presente regolamento. Sono pertanto informati dei possibili controlli tutti i soggetti di cui al precedente punto 2);
e) protezione dei dati personali: i controlli sono in ogni caso effettuati rispettando la dignità e la libertà personale dei soggetti sottoposti a controllo, nonché garantendo la riservatezza dei dati personali raccolti durante la procedura di controllo. I dati sono conosciuti soltanto dai soggetti preventivamente designati quali responsabili e incaricati del trattamento. Oltre a quanto specificato sopra, i controlli sono effettuati rispettando la normativa vigente in materia di protezione dei dati personali.

5.2 Finalità

I controlli di cui al presente regolamento sono effettuati per le seguenti finalità:

a) evitare che vengano compiuti atti e/o condotte e/o comportamenti impropri e/o potenzialmente dannosi per l'Amministrazione che possano comportare anche l'irrogazione di sanzioni disciplinari;
b) evitare o comunque ridurre i rischi di un coinvolgimento diretto e/o indiretto civile e penale dell'Azienda, per concorso di reato, nel caso di illeciti nei confronti di terzi commessi mediante l'utilizzo improprio dei beni messi a disposizione dell'Amministrazione stessa;
c) tutelare l'immagine dell'Azienda e di coloro che vi prestano la propria attività.

5.3 Modalità di effettuazione dei controlli

Il controllo è effettuato su strumentazioni informatiche determinate a seguito di specifica **segnalazione** effettuata da un soggetto terzo oppure a seguito ad una **verifica di sicurezza**.

Nel caso in cui la segnalazione del soggetto terzo si riferisca a una persona nominativamente individuata, il responsabile della sicurezza dell'Azienda deve dare informazione di tale controllo al tale soggetto, specificando che quest'ultimo può presentare richiesta di accesso ai relativi documenti amministrativi a norma della Legge n.241/1990 e succ.mod. ed int.

Le segnalazioni di un soggetto terzo sono ritenute più attendibili qualora non siano anonime e rivolte per iscritto al Responsabile della sicurezza.

La verifica di sicurezza consiste in una attività di controllo da parte del Responsabile della sicurezza, il quale, dopo aver rilevato elementi che possano configurare un utilizzo improprio delle strumentazioni informatiche, anche mediante ulteriori accertamenti, comunica i dati strettamente necessari, acquisiti attraverso tale controllo, al responsabile dell'ufficio di appartenenza del collaboratore interessato. Quest'ultimo potrà effettuare le ulteriori valutazioni e adottare le azioni conseguenti.

Gli ulteriori accertamenti sopraindicati potranno ricomprendere controlli sui log (siti di navigazione in internet). E' possibile verificare il contenuto dei siti di navigazione soltanto nel caso in cui le relative informazioni siano indispensabili al fine di rilevare un utilizzo proprio o improprio dello strumento informatico.

Qualora, anche a seguito delle ulteriori verifiche effettuate, il Responsabile della sicurezza riscontri elementi che confermino un possibile uso improprio delle strumentazioni messe a disposizione dall'Azienda, associa il nominativo dell'utilizzatore alla postazione client, per poter procedere come di seguito disciplinato.

Conseguentemente alle verifiche sopraindicate e all'individuazione del nominativo dello/degli utilizzatore/i, il Responsabile della sicurezza:

-trasmette al Dirigente un "**Verbale di controllo**" affinchè il Dirigente stesso possa effettuare le valutazioni conseguenti, con particolare riferimento ad una verifica relativa alla pertinenza (o stretta attinenza) dei dati di navigazione, trasmessi nel verbale stesso, con l'attività lavorativa;

-ne dà contestuale comunicazione al soggetto coinvolto.

La verifica di pertinenza con l'attività lavorativa, effettuata dal Dirigente, deve comprendere anche una tempestiva audizione del soggetto controllato, affinchè quest'ultimo possa fornire chiarimento, motivazioni ed osservazioni in merito a quanto rilevato. Alla audizione può essere presente, su richiesta del Dirigente, il Responsabile della sicurezza (o altro tecnico addetto alla sicurezza individuato dal Responsabile della sicurezza).

A seguito delle verifiche sopra specificate, il Dirigente comunica immediatamente per iscritto all'utilizzatore l'esito del controllo e adotta nel contempo le opportune misure tecniche/organizzative per evitare il ripetersi del comportamento anomalo.

Nel caso in cui dall'accertamento emerga un uso gravemente improprio della strumentazione informatica, il Dirigente avvia il conseguente provvedimento disciplinare.