CAMER PETROLEUM EUROPA

REGOLAMENTO AZIENDALE
PER L'UTILIZZO DELLE RISORSE INFORMATICHE

Sommario

1. Normativa di riferimento

1.1. Principali riferimenti normativi

- Decreto Legislativo 30 giugno 2003, n.196, “Codice in materia di protezione dei dati personali” e successive modificazioni e integrazioni.
- Provvedimento del Garante per la Protezione dei Dati personali del 13 ottobre 2008 “Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali”
- Legge 23 dicembre 1993 n. 547- "Modificazioni ed integrazioni alle norme del Codice Penale e del Codice di Procedura Penale in tema di criminalità informatica".
- Deliberazione 1 Marzo 2007 “Lavoro: le linee guida del Garante per posta elettronica e internet”

1.2. Violazioni della normativa

La normativa di riferimento prevede in caso di violazione sanzioni penali e amministrative.
A titolo di esempio, si elencano di seguito alcune figure di reato previste dal Codice Penale:

- Attentato a impianti informatici di pubblica utilità (art. 420);
- Falsificazione di documenti informatici (art. 491bis);
- Accesso abusivo ad un sistema informativo o telematico (art. 615ter);
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615quater);
- Diffusione di programmi diretti a danneggiare o interrompere un Sistema informativo (art. 615quinquies);
- Violazione di corrispondenza telematica (artt. 616-617sexies);
- Intercettazione di e-mail (art. 617quater);
- Danneggiamento di sistemi informatici e telematici (art. 635bis);
- Frode informatica (alterazione dell'integrità di dati allo scopo di procurarsi un ingiusto profitto) (art. 640ter).

Le seguenti figure di reato sono invece previste dal Codice Privacy:

- Trattamento illecito di dati (art. 167);
- Falsità nelle dichiarazioni e notificazioni al Garante (art. 168);
- Mancata adozione delle misure di sicurezza (art. 169);
- Inosservanza di provvedimenti del Garante (art. 170);

2. Le principali definizioni

Risorse Informatiche
Qualsiasi mezzo di comunicazione e elaborazione elettronica, hardware, software, rete, servizio e informazione in formato elettronico di proprietà di ***Camer Petroleum Europa Srl*** o in disponibilità o a essa concesso in licenza d'uso.
Le risorse informatiche includono a titolo di esempio:

- sistemi informatici ad uso amministrativo o tecnico (es. posta elettronica, accesso a Internet, applicativi aziendali ecc.)
- ogni sistema di elaborazione elettronica delle informazioni: server, personal computer fissi o portatili, tablet e similari;
- software di base e di ambiente: sistemi operativi, software di rete, sistemi per il controllo
- degli accessi, package, utility e similari;
- software di produttività individuale;
- ogni informazione elettronica registrata o conservata in file e banche dati;
- ogni periferica: stampanti, scanner, plotter, apparecchiature per l'archiviazione elettronica dei dati, supporti di memorizzazione, video terminali;
- ogni dispositivo di rete: concentratori, ripetitori, modem, switch, router, gateway, firewall, apparati VoIP e similari, access point, chiavette Internet, hard disk esterni;
- ogni mezzo trasmissivo di cablaggio strutturato per reti locali, metropolitane e geografiche:
- cavi in fibra e in rame per dorsali e cablaggio orizzontale, permutazioni, attestazioni, patch e similari.

Utilizzatori
Persone fisiche dipendenti o collaboratori a vario titolo, frequentatori che hanno accesso a strumenti informatici o telematici e che sono nella potenzialità di utilizzarli.

Trattamento
Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.
L'interessato è la persona fisica cui si riferiscono i dati personali.
In merito al tipo di dati si distinguono:

- Dato personale: Qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.
- Dato sensibile: Ogni dato personale idoneo a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.
- Dato anonimo: I dati che in origine, o a seguito di trattamento, non possono essere associati a un interessato identificato o identificabile.

In merito ai soggetti che possono effettuare operazioni di trattamento si distinguono:

- Titolare: *Camer Petroleum Europa Srl*
- Responsabile: *Dott. Giuseppe Greco*

(La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione o organismo preposti dal titolare, con atto formale di nomina, al trattamento di dati personali, sulla base di istruzioni impartite per iscritto dal titolare stesso)

- Responsabile IT ruolo: *Sig. Fabio Apollonio*

(Garantisce la pianificazione e coordina il rinnovo del sistema informatico aziendale)

- Incaricati: tutti i dipendenti degli uffici amministrativi di Camer Petroleum Europa srl: *Chirivi Giancarlo, Daniela De Razza, Nicola Conte, Valeria Negro, Vito Cardinale, Santo Palumbo, Giuseppe Melaranci, Gianluca Mungari.*

(Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile. Tipicamente gli operatori dei sistemi informatici)

Comunicazione

Il dare conoscenza dei dati personali a uno o più soggetti determinati, diversi dall'interessato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Per soggetti determinati si intendono solo i soggetti precisamente identificati e appartenenti a un elenco finito.

Diffusione

Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione. Per soggetti indeterminati si intendono soggetti non identificabili a priori.

Banca di dati

Qualsiasi complesso di dati ripartito in una o più unità dislocate in uno o più siti.

Misure minime di sicurezza

Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza, (previste nel D.Lgs. 196/2003 – Allegato B) che configurano il livello minimo di protezione richiesto per la sicurezza dei dati.

Credenziali di autenticazione

I dati e i dispositivi, in possesso di una persona, da questa conosciuti o a essa univocamente correlati, utilizzati per l'autenticazione informatica, ovvero il processo che garantisce l'accesso a un sistema informatico.
La parola chiave (password) è la componente di una credenziale di autenticazione associata a una persona e solo a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica, da mantenere riservata.

3. Premessa

Il presente documento, redatto a cura del servizio di Cyber Security aziendale, regolamenta l'accesso e l'uso delle risorse informatiche della *Camer Petroleum Europa Srl*, secondo i principi e le disposizioni della normativa citata in premessa e le indicazioni in materia di corretto uso delle risorse informatiche secondo le politiche e disposizioni aziendali definite in accordo con la Direzione aziendale.

I servizi informatici aziendali sono regolamentati, oltre che dal presente documento, dal Regolamento per l'utilizzo della Posta Elettronica e Internet. Per le misure in materia di protezione dei dati personali, ma non esclusivamente relative al trattamento di dati con supporto informatico, si rinvia ad altra documentazione aziendale specifica.

Il presente regolamento verrà aggiornato in funzione di eventuali mutamenti legislativi o in ragione di particolari necessità tecniche o organizzative. L'ultima versione del regolamento sarà sempre presente in azienda e consultabile.

4. Oggetto e campo di applicazione

Le regole stabilite si riferiscono a tutte le risorse informatiche di *Camer Petroleum Europa Srl*, devono essere applicate da tutti i soggetti che le utilizzano e hanno valenza per tutte le tipologie di dati.
Gli utenti, dipendenti e i collaboratori esterni autorizzati, devono essere nominati, ai sensi del D.Lgs. 196/2003, "incaricati del trattamento dei dati personali" a cui possono avere accesso mediante i servizi informatici aziendali.
Pertanto, i dati possono essere trattati limitatamente alle operazioni indispensabili per l'esercizio delle funzioni degli incaricati.
Gli utenti a vario titolo autorizzati devono attenersi alle disposizioni del presente regolamento.
Oltre a quanto definito in questo documento di precisa che:

- per le risorse informatiche messe a disposizione o date in uso all'azienda da altre organizzazioni valgono gli accordi e le condizioni contrattuali stipulate fra le parti;
- per l'utilizzo di dati, programmi e materiali valgono sempre le condizioni di copyright, ove previsto;
- l'utilizzo delle risorse informatiche dell'azienda deve essere comunque conforme a quanto previsto dalla normativa vigente.

5. I principali indirizzi

Le risorse informatiche:

- sono parte integrante del patrimonio dell'Azienda *Camer Petroleum Europa srl*;
- devono essere utilizzate per gestire le attività aziendali, secondo le finalità autorizzate e definite dalla Direzione Aziendale e inerenti alla propria mansione, nel rispetto dei principi di necessità, indispensabilità, non eccedenza;
- devono essere rese disponibili solo alle persone autorizzate;
- devono essere protette da danneggiamenti, furti e cause diverse che possano compromettere le attività aziendali.

6. I principali divieti

- Introdursi abusivamente nei sistemi informatici aziendali.
- Procurare a sé, o ad altri, profitto, o arrecare danni all'azienda, procurandosi, riproducendo, diffondendo, o consegnando codici, parole chiave o altri mezzi idonei all'accesso ai sistemi informatici.
- Riprodurre, copiare, duplicare e/o asportare, comunicare a terzi, diffondere i dati di cui l'azienda è titolare del trattamento.
- Riprodurre e asportare documentazione di qualsiasi tipo classificata riservata, comprese banche dati, documenti commerciali, mail aziendali se non dietro esplicita autorizzazione del titolare dei relativi diritti sia essa persona giuridica o fisica.
- Intercettare, impedire, interrompere le comunicazioni inerenti ai sistemi informatici.
- Distruggere, deteriorare, rendere inservibili, del tutto o in parte, i sistemi informatici ovvero i programmi e le informazioni o i dati esistenti nei sistemi.
- Riprodurre, duplicare e/o asportare programmi installati di cui l'azienda è licenziataria o proprietaria.
- Introdurre, installare, utilizzare programmi che non siano stati regolarmente acquistati, distribuiti e installati dalle preposte funzioni aziendali.
- Adottare comportamenti che mettano a rischio la sicurezza del sistema informatico/informativo, inclusi i dati contenuti, o che pregiudichino o ostacolino le attività della collettività degli utilizzatori.

7. Responsabilità

7.1. Procedure informatizzate autorizzate

Le procedure informatiche distribuite e gestite dall'IT interno aziendale sono tutte e solo quelle individuate nell'Allegato A - Elenco Applicativi di base e specifici autorizzati.
Tale allegato sarà costantemente aggiornato dall'IT e sempre disponibile. Relativamente a tali procedure, sono a carico dell'IT le misure di sicurezza, e più in generale il rispetto della normativa e delle disposizioni aziendali, per quanto riguarda i server, i software di base, le procedure applicative in ambito amministrativo, le infrastrutture, i dispositivi della rete aziendale.
Infine, sono a carico degli utilizzatori (responsabili del trattamento e incaricati, ciascuno per i rispettivi ambiti di competenza e responsabilità) le misure di sicurezza, e più in generale il rispetto della normativa e delle disposizioni aziendali, in particolare questo regolamento, per quanto riguarda le postazioni di lavoro (Personal Computer) e le attività svolte con esse.

7.2. Procedure informatizzate non gestite dall' IT

Fermo restando il divieto di utilizzare programmi non autorizzati, se per qualsiasi ragione, in particolare la necessità di garantire la continuità operativa, dovessero essere in uso presso le Unità Operative procedure informatizzate NON distribuite dall'IT, fintanto che esse rimangono operative l'organizzazione e la gestione delle misure di sicurezza, e più in generale il rispetto della normativa e delle disposizioni aziendali, sono a carico del singolo responsabile del trattamento, che deve rivolgersi all'IT per verificarne la corretta applicazione.

8. Sistemi di autenticazione e di autorizzazione

Il responsabile del trattamento, individuati gli incaricati, dovrà richiedere l'attivazione della credenziale di autenticazione informatica, specificando a quali dati e tipi di operazioni può accedere in relazione ai compiti impartiti.
Il trattamento di dati personali, con strumenti elettronici, è consentito infatti ai soli incaricati dotati di credenziali di autenticazione, in genere costituite da Nome Utente (username) e password.

8.1. Credenziali di autenticazione (coppia username e password)

Le credenziali di autenticazione sono il presupposto necessario per l'utilizzo dei sistemi informatici messi a disposizione da *Camer Petroleum Europa Srl*. Le credenziali consentono il superamento di una procedura d'autenticazione che permette l'accesso a uno specifico trattamento o a un insieme di trattamenti.

8.2. Rilascio e rinnovo delle credenziali

Tutte le informazioni relative alle modalità di rilascio e di rinnovo delle credenziali sono riportante nell'Allegato B - Istruzioni per il rilascio e il rinnovo di credenziali aziendali a personale dipendente e non dipendente.

8.3. Gestione delle credenziali

Le credenziali possono consistere:

- in un codice per l'identificazione dell'incaricato, associato ad una parola chiave riservata conosciuta solamente dal medesimo (**username e password**),
- in un dispositivo d'autenticazione (per es. una carta magnetica o smart card) in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave,
- in una caratteristica biometrica dell'incaricato (per es. impronta digitale), eventualmente associata a un codice identificativo o a una parola chiave.

Lo ***username***, o nome utente, è di norma costituito dal nome e dal cognome dell'utilizzatore intervallati da un "**.**" (ad esempio: **mario.rossi**).
Lo stesso username non potrà, neppure in tempi diversi, essere assegnato a incaricati diversi.
La ***password*** (o parola chiave) è una parola segreta, conosciuta solo dall'incaricato che, in coppia con lo username, permette di accedere alla procedura informatizzata scelta dal dipendente e deve essere cambiata, per motivi di sicurezza, ogni qualvolta il responsabile del trattamento dei dati lo richieda (con altra diversa da quella precedente).
La password è strettamente personale e per nessun motivo deve essere resa nota ad altri. La sua conoscenza da parte di estranei consentirebbe il trattamento dei dati per nome e per conto del possessore delle credenziali. Infatti, l'eventuale uso improprio di apparecchiature, strumenti o servizi sarà imputato al titolare della password con la quale è avvenuto l'accesso.
A ogni incaricato sono assegnate individualmente una o più credenziali per l'autenticazione. L'assegnatario dovrà farne un uso strettamente personale (quindi non condivisibile con altri), operare nell'ambito delle autorizzazioni ricevute e utilizzare le risorse solo per scopi aziendali.
Ogni incaricato è tenuto ad adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale (password), e la diligente custodia dei dispositivi in suo possesso o a suo uso esclusivo.
Le credenziali vengono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali. (ad es. licenziamento o dimissioni volontarie)
Sono esplicitamente vietate credenziali di accesso anonime, ovvero non corrispondenti a una persona fisica.
La scelta sicura della password si realizza attraverso le seguenti regole di buon senso:

- deve essere facilmente memorizzabile in modo tale che si possa evitare di scriverla (per es. sulla postazione di lavoro o in prossimità), ma non banale e di facile individuazione (per es. con riferimenti chiari all'incaricato). La sua lunghezza deve essere di almeno otto caratteri e deve contenere almeno un numero e una lettera maiuscola.
- deve essere modificata ogni volta che si abbia la sensazione che possa essere conosciuta, intenzionalmente o accidentalmente, da altri.
- in caso di modifica, la nuova password non deve essere uguale a una password già usata in precedenza.

8.4. Sistema d'autorizzazione per le procedure informatizzate distribuite dall'IT

L'assegnazione di credenziali di autenticazione del tipo "nome.cognome" abilita l'assegnatario a una serie di "servizi informatici di base" quali a esempio:

- accesso a una casella di posta elettronica;
- visualizzazione del portale del dipendente su Cronos;
- accesso a Internet;
- accesso a una cartella di rete personale (se richiesta);
- accesso potenziale a gran parte degli applicativi aziendali (richiede separata autorizzazione).

L'abilitazione all'uso dei servizi informatici di base può essere richiesta all'IT direttamente dall'interessato.
Per l'abilitazione all'accesso a servizi informatici e procedure non comprese nei servizi di base, la relativa autorizzazione dovrà essere richiesta dal responsabile della struttura organizzativa di appartenenza al responsabile del Trattamento tramite l'IT.
È dovere del responsabile di una struttura organizzativa, firmatario della suddetta modulistica, dare immediata comunicazione all'IT circa la modifica o revoca di funzioni che avevano giustificato l'accesso da parte di un proprio collaboratore a procedure/banche dati/servizi.
La richiesta di modifica o disattivazione di un profilo deve pervenire con almeno 10 giorni d'anticipo rispetto alla data di variazione.

La maggior parte dei servizi e procedure informatiche distribuite dall'IT prevedono differenti profili di autorizzazione: tali profili, definibili per ciascun incaricato o per classi omogenee d'incaricati,

devono essere individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
Periodicamente, e comunque almeno annualmente, il responsabile del trattamento deve verificare la sussistenza delle condizioni per la conservazione dei profili d'autorizzazione attribuiti ai singoli incaricati. Per semplificare tale attività, il SIM renderà periodicamente disponibili gli elenchi degli utenti con le abilitazioni e i profili assegnati, relativamente alle principali procedure informatiche aziendali.
Dopo un limitato numero di tentativi d'accesso falliti, alcuni sistemi di sicurezza disattivano lo username, che sarà riattivabile solo a seguito di richiesta scritta del singolo incaricato del trattamento.
Nel caso di prolungata assenza o impedimento di un incaricato le cui credenziali consentano in modo esclusivo l'accesso ad alcuni dati o strumenti elettronici, tale da rendere indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, l'incaricato potrà individuare per iscritto un altro lavoratore (fiduciario) a cui affidare il compito dell'accesso in sua vece, o, alternativamente, il Responsabile del trattamento potrà richiedere per iscritto all'IT di autorizzare un altro incaricato all'accesso ai dati o strumenti interessati. Tale attività dovrà essere riportata in apposito verbale dal Responsabile che deve informare l'incaricato del trattamento alla prima occasione utile.

9. Norme generali per l'utilizzo delle apparecchiature informatiche

L'utente deve utilizzare in modo corretto e lecito le risorse che gli sono state messe a disposizione. Si riportano di seguito alcune tra le principali indicazioni a cui gli utilizzatori sono tenuti ad attenersi; l'IT è a disposizione per fornire chiarimenti e ulteriori precisazioni in merito ad aspetti che possano risultare complessi o troppo tecnici.

9.1. Computer aziendali

Il personal computer aziendale in dotazione è uno strumento di lavoro. L'utilizzo personale o improprio dello stesso può comportare inefficienze, problemi di sicurezza e costi di manutenzione imprevedibili ed è pertanto non consentito, salvo casi particolari espliciti.
Il computer deve essere usato in condizioni di sicurezza e stabilità che lo preservino da pericoli di danneggiamento.
Possono essere utilizzati unicamente programmi/applicazioni installati o autorizzati dall'IT e per i quali siano stati regolarmente assolti gli oneri relativi alla concessione delle licenze d'uso, ove richieste. In caso di necessità di ulteriori applicazioni il dipendente dovrà farne richiesta all'IT.
È vietato disinstallare o disattivare i software presenti sul PC, in particolare i sistemi di protezione e sicurezza aziendali (tra cui l'antivirus), e i prodotti software di inventariazione e controllo remoto (OCS Inventory, UltraVNC ecc.). Eventuali eccezioni devono essere concordate con l'IT ed esplicitamente autorizzate.
Il personale tecnico potrà effettuare verifiche automatizzate o puntuali sui software presenti nelle postazioni, rimuovendo o bloccando l'esecuzione dei software non autorizzati, richiedendo eventualmente giustificazioni agli utenti utilizzatori relativamente alle anomalie riscontrate.
L'utilizzatore è personalmente responsabile del computer assegnatogli; egli ha pertanto l'obbligo, per quanto nelle sue possibilità, di impedire ad altri indebiti utilizzi dell'apparecchiatura informatica.
Si sottolinea che il furto o l'indebito utilizzo di un computer rilevano, oltre che sotto il profilo patrimoniale, anche in relazione a un possibile improprio utilizzo dei dati in esso contenuti e/o alla perdita degli stessi.
È obbligatorio segnalare tempestivamente casi di furti o incidenti relativi alla sicurezza.

Per finalità di sicurezza e risparmio energetico, computer e monitor devono sempre essere spenti al termine del loro utilizzo. Le apparecchiature devono essere disattivate anche nel caso di prolungate assenze dal servizio, pur nell'ambito dell'orario di lavoro.

In caso di assenze brevi (es. pausa mensa, riunione ecc.) durante le quali l'apparecchiatura rimane incustodita è obbligatoria l'attivazione dello screen saver (salvaschermo) protetto da password. Al computer possono essere connesse solamente periferiche o dispositivi forniti o autorizzati dall'Azienda, da utilizzarsi esclusivamente se necessari per le attività aziendali.
Nessuna periferica o dispositivo componente la stazione di lavoro può essere rimossa, salvo specifica autorizzazione.
Il personale tecnico della *Camer Petroleum Europa Srl* potrà effettuare verifiche automatizzate o puntuali sulle periferiche presenti nelle postazioni, disabilitando o rimuovendo le periferiche non autorizzate, eventualmente chiedendo motivazioni e giustificazioni agli utenti utilizzatori relativamente alle anomalie riscontrate.

9.2. Computer portatili e aziendali

Oltre a quanto indicato nel paragrafo precedente, gli utilizzatori dei computer portatili aziendali (includendo anche tablet, mini PC ecc.) devono seguire le seguenti istruzioni.
Il computer portatile deve essere conservato con cura sia durante gli spostamenti sia sul luogo di utilizzo aziendale o extraaziendale, adottando idonee precauzioni per preservarlo da furti e custodendolo in luogo sicuro in caso di allontanamento, anche temporaneo.
Inoltre, in luoghi pubblici non devono essere inserite o lette informazioni di carattere riservato o critico.

9.3. Utilizzo di attrezzature informatiche personali

Le attrezzature personali di qualsiasi tipologia (PC, tablet, smartphone ecc.) non possono essere collegate alla rete aziendale, salvo diversa esplicita autorizzazione in forma scritta.
In alcuni casi i dispositivi personali potranno collegarsi a sottoreti appositamente predisposte nel rispetto della sicurezza della rete aziendale e pertanto destinate a funzioni limitate (es. rete ospiti per accesso a Internet).

9.4. Stampanti e scanner

Salvo eccezioni particolari e giustificate (es. ambulatori, guardiole, sportelli), saranno sempre installate stampanti di rete o fotocopiatrici multifunzione (con funzione stampante e scanner) in modo da consentirne l'uso condiviso tra più uffici, settori, strutture, anche al fine di un razionale utilizzo delle risorse assegnate.
È consentita la stampa solo di documenti strettamente necessari, mentre dovrà essere privilegiato l'utilizzo di documenti informatici. In caso di stampa è importante ritirarla prontamente dai vassoi delle stampanti comuni per evitare accesso indesiderato a dati personali. Si raccomanda in particolare di indirizzare verso una stampante dedicata, collocata in un'area controllata, le stampe di dati sensibili.
È buona regola, inoltre, privilegiare la stampa di documenti in modalità fronte/retro e bianco/nero in *modalità risparmio*.
Nell'utilizzo dello scanner accertarsi di utilizzare sempre una bassa risoluzione di scansione, in particolare prima di inviare, per es. via mail, un documento scansionato.
Si ricorda che nel caso di utilizzo di scanner deve essere rispettata la normativa sul diritto d'autore, analogamente a quanto avviene per la riproduzione di documenti attraverso fotocopiatrici.
Inoltre non possono essere scansionati documenti aventi contenuto oltraggioso e/o discriminatorio per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

9.5. Supporti di memorizzazione: CD, DVD, hard disk esterni, memory card, pen drive

L’utilizzo di hard disk esterni e supporti di memorizzazione rimovibili deve essere effettuato con molta cautela, utilizzando solo dispositivi necessari per le attività aziendali e di proprietà aziendale. Al momento della connessione di un dispositivo esterno viene avviata la scansione automatica anti-malware, che non può essere interrotta dall’utente per permettere al sistema di sicurezza di completare la verifica. È inoltre fondamentale che il dispositivo non venga disconnesso durante la scansione, manovra che rischia di danneggiare e rendere non più leggibili i dati presenti sul dispositivo.
È da evitare il salvataggio su tali supporti di dati sensibili. Infatti, l’eventuale perdita accidentale del supporto consentirebbe a chiunque di accedere ai medesimi dati, senza che peraltro si conosca la sua identità.
Nel caso fosse strettamente necessario, per es. se il dispositivo è utilizzato per le copie di sicurezza, è obbligatorio criptare i dati con programmi adeguati, in genere già contenuti negli stessi supporti. Per eventuali istruzioni rivolgersi al personale tecnico.
L'utilizzo di dispositivi rimovibili, utile per esempio per effettuare copie di sicurezza o per trasportare file di grandi dimensioni, rimane in ogni caso sotto l’esclusiva responsabilità dell'utilizzatore e deve essere effettuato avendo cura di cifrare i dati aziendali riservati e i dati personali o sensibili con l'utilizzo di password sicure.
Alcune raccomandazioni di buon senso:

- I supporti rimovibili (CD, DVD, pen drive, memorie flash per macchine fotografiche digitali e palmari, hard disk rimovibili ecc.) devono essere custoditi con la massima riservatezza e con la massima diligenza e non devono essere lasciati incustoditi o facilmente accessibili da parte di altri incaricati non autorizzati al trattamento dei dati contenuti.
- In particolare, durante il loro utilizzo devono essere presidiati dagli incaricati e quando non temporaneamente utilizzati devono essere riposti in contenitori sicuri.
- I supporti rimovibili possono essere utilizzati e ceduti solamente tra gli incaricati autorizzati al trattamento dei dati in essi contenuti.
- I supporti rimovibili non riscrivibili, per i quali i dati presenti non possono essere eliminati attraverso procedure di formattazione del supporto (ad esempio: CD-R, DVD-R, DVD+R ecc.), devono essere distrutti fisicamente nel momento in cui si ritiene non debbano essere più utilizzati per il trattamento.
- I supporti rimovibili riscrivibili (ad esempio: CD-RW, DVD-RW, DVD+RW, pen drive, memorie flash per macchine fotografiche digitali e palmari, hard disk rimovibili ecc.) non più utilizzati per il trattamento di dati devono essere formattati completamente e a basso livello da parte degli utilizzatori, in modo che i dati precedentemente in essi contenuti non siano intelligibili e non siano tecnicamente in alcun modo ricostruibili.

È vietato consegnare a terzi supporti in precedenza utilizzati per la memorizzazione di dati personali o sensibili, anche se cancellati, in quanto è tecnicamente possibile il loro recupero anche dopo la cancellazione.

L’utente è tenuto a comunicare immediatamente al proprio Responsabile o a denunciare all’autorità giudiziaria l’eventuale furto, smarrimento, perdita ovvero appropriazione a qualsivoglia titolo da parte di terzi dei supporti rimovibili. Copia della denuncia deve essere consegnata tempestivamente al responsabile del Trattamento dei dati.

È infine obbligatorio verificare sempre l’assenza di virus prima dell’utilizzo dei supporti rimovibili.

9.6. Norme generali per l’utilizzo del software distribuito dall’IT

L’incaricato del trattamento:

- deve utilizzare il software solo per attività aziendali;
- deve custodire il software ricevuto in dotazione;
- non deve cedere il software a colleghi o a terzi;
- deve utilizzare solo il software aziendale assegnato.

Inoltre si ribadisce che:

- è vietata qualsiasi riproduzione (permanente, temporanea, parziale o totale), traduzione, distribuzione di software di terzi, che non sia autorizzata in base alla licenza a esso applicabile,
- salvo specifiche autorizzazioni, non è consentito l'uso in azienda di software acquisito privatamente o disponibile gratuitamente, né l'uso all'esterno dell'azienda di software aziendale.

9.7. Software antivirus e di protezione dei dati

L'IT, mediante l'utilizzo di firewall e prodotti antivirus gestiti e aggiornati centralmente, assicura la protezione dell'infrastruttura, dei sistemi informatici e delle postazioni di cui effettua la manutenzione.
L'aggiornamento dell'antivirus avviene giornalmente, quello delle patch critiche e di sicurezza di Windows avviene mensilmente, previa verifica in ambienti di test.
È comunque responsabilità di ogni incaricato controllare che il PC sia dotato del prodotto antivirus aziendale e che sia configurato per l'aggiornamento automatico. In caso contrario l'incaricato è tenuto a farne immediata richiesta all'IT.
È vietato il collegamento alla rete aziendale di qualsiasi personal computer non adeguatamente protetto mediante software antivirus (aggiornamento almeno settimanale) e patch di sicurezza del sistema operativo (aggiornamento almeno mensile).

9.8. Dischi di rete, cartelle personali e cartelle condivise

Camer Petroleum Europa Srl mette a disposizione degli utilizzatori che ne fanno richiesta, dischi di rete (cartelle che possono essere personali o condivise tra più utilizzatori) per l'archiviazione di informazioni di carattere professionale. Non possono essere collocati sulle unità di rete - nemmeno per periodi brevi - file personali o comunque aventi contenuto diverso da quello strettamente connesso all'attività lavorativa.
La richiesta di attivazione di tale servizio va fatta tramite il Modulo per l'utilizzo dei Servizi Informatici Aziendali (vedi anche Allegato B).
L'IT deve svolgere periodici controlli a campione sulle unità di rete e può procedere autonomamente alla rimozione di dati non connessi alle attività proprie dell'azienda. Nel caso in cui la natura o il contenuto di informazioni/dati da collocare in rete per un utilizzo professionale potesse risultare dubbia/ambigua il titolare degli stessi dovrà informare preventivamente l'IT affinché non proceda alla rimozione.
L'IT provvede al backup dei dati collocati su unità di rete. Nel caso di perdita di dati in rete, pertanto, sarà possibile richiedere il recupero del file così come salvato nell'ultima versione di backup. Per questi motivi è fortemente consigliato l'utilizzo delle unità di rete per il salvataggio di dati/file di particolare importanza e rilevanza.
Le unità di rete devono essere mantenute con diligenza a cura degli utilizzatori; agli stessi è richiesta la periodica – almeno semestrale – revisione dei dati salvati e l'eliminazione di quelli obsoleti o, comunque, non più utilizzati o necessari. È opportuno evitare la duplicazione di dati onde consentire uno sfruttamento razionale delle unità di rete. I server aziendali centralizzati sono le uniche entità predisposte alla condivisione di risorse. È vietato condividere localmente e direttamente dischi, cartelle o risorse (es. cartelle di scambio) a eccezione delle stampanti comuni.
Solo in situazioni di particolari problematiche tecniche, su autorizzazione dell'IT, potranno essere attivate condivisioni fra personal computer che dovranno inderogabilmente essere protette da password di accesso.
Per ogni cartella condivisa è individuato un referente, avente la responsabilità di definire l'elenco degli utilizzatori e dei profili di abilitazione, nonché di verificare il corretto utilizzo della cartella da parte degli utilizzatori stessi.

Al referente spetta verificare periodicamente e comunque almeno annualmente, le abilitazioni assegnate agli utilizzatori, segnalando tempestivamente al SIM la necessità di assegnare, modificare o cancellare l'accesso alla cartella da parte degli utilizzatori.

Il referente della cartella più individuare fino a 2 collaboratori per affiancarlo nella gestione delle abilitazioni all'uso della cartella.
Lo spazio assegnato può essere concordato di volta in volta secondo le reali necessità.

9.9. Presentazioni

È fatto divieto di inserire dati personali nelle presentazioni (es. Power Point): si devono utilizzare dati privi di qualsiasi riferimento ai soggetti interessati. Va precisato che anche codifiche, quali il codice fiscale o altro codice, non sono ammesse in quanto possono ricondurre indirettamente ai dati identificativi del soggetto interessato.

10. Collegamento di attrezzature alla rete dati

La rete dati aziendale su cavo o wireless (wi-fi) è gestita dall'IT.
L'accesso di computer o altre attrezzature alla rete aziendale deve essere autorizzato dall'IT, che definisce la connettività da assegnare in base alle caratteristiche dell'attrezzatura e alle esigenze dell'utilizzatore.

10.1 Rete Aziendale

La rete interna permette l'accesso a tutti i principali applicativi aziendali e pertanto è destinata all'uso da parte dell'utente aziendale esclusivamente mediante dispositivi dell'azienda.
Il collegamento alla rete di attrezzature informatiche personali, se ammesso, è regolato mediante accesso a sottoreti predisposte ad-hoc (per es. la rete ospiti per l'eccesso a internet).
Pertanto, sono vietati:

- Il collegamento alla rete aziendale di computer e server se non forniti o autorizzati dall'IT.
- Il collegamento alla rete aziendale di personal computer non adeguatamente protetti mediante software antivirus (aggiornamento almeno settimanale) e patch di sicurezza del sistema operativo (aggiornamento almeno mensile).
- Il collegamento alla rete, non autorizzato dall'IT, di apparati di rete quali switch, router
- (anche USB o wi-fi) e attrezzature per reti wireless (es. access point).
- Qualsivoglia forma di collegamento ad altre reti laddove la stazione di lavoro sia connessa alla rete aziendale *Camer Petroleum Europa Srl*; sono pertanto vietate, per le stazioni di lavoro connesse alla rete aziendale, le connessioni tramite modem o chiavette Internet e l'utilizzo di una doppia scheda di rete; per i PC portatili dotati sia di scheda di rete tradizionale che di scheda di rete wireless, entrambe le schede possono essere abilitate al collegamento alla rete aziendale purché non vengano utilizzate contemporaneamente.

11. Uso e salvataggio dei dati aziendali

L'IT provvede al salvataggio dei dati registrati tramite i sistemi informativi aziendali centralizzati. La politica di backup (creazione di copie di sicurezza), che definisce la frequenza di salvataggio e il tempo di tenuta dei backup, viene adottata dall'IT in linea con indicazioni normative, raccomandazioni e best practices.
Al fine di salvaguardare tutti gli altri dati aziendali ritenuti di interesse e utilità per *Camer Petroleum Europa Srl* (es. documenti .doc, .xls, .pdf, ecc.), **è vietato memorizzarli sull'hard disk dei PC**: a tale scopo dovranno invece essere utilizzati i server gestiti dall'IT (vedi capitolo "Dischi di rete, cartelle personali e cartelle condivise.
Nel caso invece sia indispensabile memorizzare dati aziendali localmente sugli hard disk dei PC, è fatto obbligo agli utenti di effettuare una copia di sicurezza di tali dati, con frequenza almeno settimanale.

L'IT a questo scopo fornisce, su richiesta, i dispositivi hardware necessari per il salvataggio dei dati su supporto rimovibile. È fondamentale che tali supporti non siano permanentemente accessibili dal PC onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza: a tal fine si raccomanda di collegare i dispositivi di backup solo per il tempo strettamente necessario alla realizzazione della copia di sicurezza, rimuovendoli opportunamente al termine della copia e riponendoli in luogo sicuro. Vedi anche paragrafo "Supporti di memorizzazione: CD, DVD, hard disk esterni, memory card, pen drive".
È responsabilità degli utenti conservare adeguatamente e proteggere le copie di backup.

12. Norme generali per l'utilizzo dei servizi Internet

12.1. Posta elettronica e navigazione Internet

Relativamente al corretto utilizzo della posta elettronica e della rete Internet si rinvia al relativo regolamento.

12.2. Pubblicazione di contenuti e realizzazione di siti personali

L'utente non è autorizzato in alcun caso a produrre e a pubblicare siti web personali utilizzando risorse aziendali né a pubblicare autonomamente siti riferiti alla struttura di appartenenza.
Ogni eventuale necessità di realizzare siti web personali o di struttura utilizzando risorse aziendali dovrà essere espressamente autorizzata dal responsabile aziendale del Trattamento.
È fatto divieto agli utenti di utilizzare il logo aziendale nei siti personali senza autorizzazione del responsabile del trattamento dei dati.
È fatto divieto agli utenti di inserire nei siti personali collegamenti (link) al sito aziendale senza autorizzazione dell'IT.
È fatto assoluto divieto di realizzare funzioni di Hosting utilizzando risorse aziendali.

12.3. Connessione a provider diversi da quello aziendale

È vietato l'utilizzo di accessi internet mediante Internet Provider diversi da quello aziendale e la connessione di stazioni di lavoro aziendali alle reti di detti Provider, anche con abbonamenti privati.
Infatti tali connessioni rappresentano un potenziale rischio per la sicurezza dell'intero sistema informativo aziendale di cui l'utente è pertanto consapevole.

12.4. Utilizzo di server esterni per backup/gestione/condivisione documenti aziendali

È vietato caricare documenti aziendali riservati e dati sensibili su sistemi di memorizzazione esterni cloud quali Dropbox, Google Drive, SkyDrive, ICloud ecc.
Ciò in quanto tali sistemi possono essere soggetti ad attacchi informatici e i dati possono essere sottratti o manipolati illegalmente. Inoltre, molti di tali sistemi sono ospitati in paesi non soggetti a regolamentazioni sulla privacy analoghe a quella italiana. Non verranno pertanto effettuate abilitazioni specifiche che permettano la connessione a tali sistemi, salvo casi particolarissimi da valutare e autorizzare singolarmente (per es. accessi temporanei per prelevare dati da gruppi di lavoro già esistenti).

12.5. Assistenza da remoto (VPN e altre tipologie)

Sono ammessi collegamenti remoti dall'esterno per l'accesso alle risorse aziendali, sia per manutenzione di attrezzature da parte di ditte esterne, sia per lo svolgimento di specifiche attività da una sede esterna, ma devono essere autorizzati dall'IT.

13. Modalità di prestazione dei servizi

L'IT si impegna a fornire continuità ai servizi erogati, riservandosi la possibilità di interromperli esclusivamente per le manutenzioni ordinarie e cercando di arrecare il minor disagio possibile agli utilizzatori. Salvo impedimenti le interruzioni saranno comunicate agli utenti.
Per poter fornire assistenza e supporto tempestivi nel caso di guasti e malfunzionamenti, su ciascun computer fisso o portatile è installata un'applicazione che consente all'IT di collegarsi remotamente, senza bisogno di intervenire sul luogo.
Pertanto, la manutenzione alle stazioni di lavoro viene generalmente effettuata, in prima battuta, mediante tali sistemi software di manutenzione remota. Solo nel caso di mancata soluzione del problema in modalità remota, viene effettuato un intervento in loco.
Si informa che i sistemi di controllo remoto suddetti sono configurati affinché l'operatore che interviene per la manutenzione possa farlo esclusivamente previo consenso dell'utilizzatore della postazione (consenso che viene richiesto in tempo reale sullo schermo del pc); non sarà richiesta l'autorizzazione solo nei casi in cui si renda necessario effettuare installazioni o aggiornamenti software da remoto, che non prevedono la possibilità di accesso ai dati presenti.
Inoltre, l'utente può verificare l'attività effettuata in remoto dal tecnico rimanendo presso la postazione.
Gli interventi sono eseguiti da personale identificato e autorizzato dal responsabile del Trattamento e cioè dall'IT.

14. Disposizioni finali

14.1. Cessazione della disponibilità dei servizi informatici aziendali

Ai sensi del presente regolamento, la disponibilità a un utente dei servizi informatici aziendali cesserà totalmente nel caso non sussista più la condizione di dipendente o di collaboratore esterno; inoltre può cessare o essere limitata nei privilegi assegnati in caso di:

- revoca dell'autorizzazione all'uso fornita dal Responsabile (per es. per cambio di mansione, ruolo, CDR ecc.);
- accertato uso non corretto o comunque estraneo alla sua attività lavorativa dei servizi informatici aziendali;
- accertate manomissioni e/o interventi illeciti sul hardware e/o sul software;
- accertate diffusione o comunicazione imputabili direttamente o indirettamente all'utente, di password, procedure di connessione, indirizzo I.P. e altre informazioni tecniche riservate;
- accesso illecito e intenzionale dell'utente a directory, a siti e/o file e/o servizi da chiunque resi disponibili, in particolare se l'attività dell'utente comporti danno, anche solo potenziale al sito contattato;
- violazione delle regole essenziali stabilite dal presente regolamento.

Si precisa che in caso di cessazione della condizione di dipendente o collaboratore a una certa data la casella di posta dell'utente sarà immediatamente bloccata. A partire da tale data non sono consentiti né l'accesso alla casella, né la ricezione tramite inoltro.
Casi particolari devono essere esplicitamente autorizzati dalla Direzione Aziendale.
Si ricorda inoltre che, una volta cessata la condizione di dipendente o collaboratore è vietato asportare dati aziendali prodotti nell'attività istituzionale. Non sarà dato seguito, pertanto, alla richiesta di scarico massivo (per es. su supporto esterno) delle mail dell'utente, né di altri file contenuti nei file server o nei personal computer.

14.2. Responsabilità dell'utilizzatore delle risorse informatiche

L'utente è direttamente e totalmente responsabile dell'uso che egli fa del servizio di posta elettronica e di accesso a Internet, dei contenuti che vi ricerca, dei siti che contatta, delle informazioni che vi immette e delle modalità con cui opera.
All'utente è consentito di utilizzare il servizio solo per ragioni professionali connesse alla propria attività, in modo individuale, salvo eccezioni riportate del relativo regolamento.
Con l'accettazione di questo regolamento l'utente è informato e consapevole del fatto che la conoscenza della password da parte di terzi consente a questi ultimi l'accesso alla rete aziendale e l'utilizzo dei relativi servizi in nome dell'utente e l'accesso ai dati cui il medesimo è abilitato, con le conseguenze che la cosa può comportare, quali ad esempio la visualizzazione di informazioni riservate, la distruzione o la modifica dei dati, la lettura della propria posta elettronica, l'uso indebito di servizi ecc.
L'utente prende atto che è vietato servirsi o dar modo ad altri di servirsi della rete aziendale e dei servizi da essa messi a disposizione per utilizzi illeciti che violino o trasgrediscano diritti d'autore, marchi, brevetti, comunicazioni private o altri diritti tutelati dalla normativa corrente, per utilizzi contro la morale e l'ordine pubblico, per recare molestia alla quiete pubblica o privata, per recare offesa o danno diretto o indiretto all'Azienda o a terzi.

14.3. Informativa sul trattamento dei dati da parte del SIM

Ai sensi dell'art. 13 del D. Lgs. n. 196/2003 e s.m. si informa che i dati relativi all'utilizzo dei servizi informatici da parte degli utenti sono trattati nel rispetto della legge e degli obblighi di riservatezza cui è ispirata l'attività dell'Azienda.
Il trattamento dei dati si svolge nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza e all'identità personale e al diritto di protezione dei dati personali.

Finalità e modalità del trattamento
Camer Petroleum Europa Srl si impegna a trattare i dati relativi all'utilizzo dei servizi informatici unicamente per motivi volti a garantire la sicurezza e il corretto funzionamento dei servizi informatici e per finalità direttamente pertinenti all'attività lavorativa del dipendente.
Le operazioni effettuate servendosi delle credenziali di autenticazione potranno essere memorizzate per finalità di sicurezza del sistema.
L'attività di registrazione avviene attraverso i file "log" di sistema a cura del Responsabile IT o dell'articolazione aziendale che detiene la responsabilità organizzativa dei sistemi o servizi.
Per quanto riguarda l'utilizzo dei sistemi informativi aziendali, le operazioni effettuate servendosi delle credenziali di autenticazione potranno essere memorizzate al fine di garantire la tracciabilità del trattamento dei singoli dati. Le informazioni relative alla tracciabilità del dato (inserimento, modifica, cancellazione) vengono gestite con le stesse modalità del dato a cui si riferiscono.
Per quanto riguarda l'accesso ai servizi di posta elettronica e internet, l' IT garantisce la custodia dei file "log" per trenta mesi o comunque per il tempo indicato da fonti normative o regolamentari.
Le registrazioni potranno essere utilizzate, su richiesta del Titolare o dei Responsabili del trattamento dei dati personali, per finalità statistiche e di valutazione della qualità in riferimento a taluni servizi erogati, esclusivamente da parte del personale dell'Azienda sotto la diretta responsabilità dell'IT.
Camer Petroleum Europa Srl si riserva di effettuare dei controlli, anche a campione, concernenti l'utilizzo corretto degli strumenti di lavoro, fermo restando il divieto di controllo a distanza dei lavoratori stabilito dall'art. 4 della L. 20.5.1970, n. 300.

Comunicazione e diffusione
I dati relativi all'utilizzo degli strumenti informatici sono trattati, per le finalità indicate al punto precedente, dal Responsabile IT e possono essere portati a conoscenza, esclusivamente nei casi consentiti dalla legge, del responsabile trattamento dei dati. Infine, i log potranno essere oggetto

di provvedimenti dell'Autorità giudiziaria e amministrativa e in generale dei soggetti aventi funzioni ispettive e di controllo all'interno dell'Azienda.

Titolarità

Il Titolare del trattamento dei dati è la *Camer Petroleum Europa Srl*, legalmente rappresentata dall'Amministratore pro-tempore Avv. Sonia Greco, con sede legale in Galatina alla s.p. 362 (ex s.s.476) Galatina LE.
L'Amministratore ha nominato Responsabile del trattamento il **Dott. Giuseppe Greco** e IT il **Sig. Fabio Apollonio.**

Diritti dell'utente "interessato"

A seguito del trattamento dei dati, si possono esercitare i diritti previsti ai sensi dell'art.7 del D.Lgs. n. 196/03, e più precisamente l'utente, in qualità di "interessato", può conoscere i dati trattati, nonché può richiedere l'aggiornamento, la rettifica e, ove abbia interesse, l'integrazione, nonché le altre prerogative previste dalla Legge. È possibile in qualsiasi momento far valere i diritti di cui all'art. 7 con richiesta avanzata al Titolare o al responsabile del Trattamento dei dati.

Allegato A – Elenco applicativi di base e specifici autorizzati

Applicativi di base (sono esclusi dall'elenco i sistemi operativi)

#	Applicativi di base	Note
AB1	Kaspersky antivirus	10.2.6.3733 - 10.3.0.6294
AB2	UltraVnc	1.0.9.5
AB3	Oracle 8.1.7 ADS/9/10g/11g	Oracle 8.1.7/9/10g/11gR2
AB4	Java Runtime Environment 1.6 update 25 o 1.7 update 09	La versione dipende dal tipo di applicativi installati
AB5	.Net Framework 3.5 Sp3	Su Windows 10 .Net framework 4.0
AB6	Oracle Jinitiator	1.3.1.22
AB7	Adobe Reader	7 – 8 – 9 – 10 - 11
AB8	PdfCreator	8.2.0
AB9	Peazip	3.1
AB10	CdburnerXp	4.5.8
AB11	Vlc	2.2.4
AB12	LibreOffice	4.4.2
AB13	Open VPN	2.4.3
AB15	Mozilla Firefox 41 o superiore	41.0.2
AB16	Google Chrome	59

Allegato B

Istruzioni per il rilascio e il rinnovo di credenziali aziendali a personale dipendente e non dipendente

Per accedere ai servizi informatici aziendali qualsiasi nuovo utente dovrà fornire i propri dati personali, prendere visione del presente regolamento e compilare il modulo per l'utilizzo dei servizi informatici aziendali.
Il modulo dovrà essere consegnato alla struttura aziendale deputata alla creazione degli accessi ai sistemi o servizi di cui si richiede l'abilitazione (corrispondente all'IT nella maggioranza dei casi), firmato dal Responsabile del trattamento dei dati personali.
L'utilizzo dei servizi informatici aziendali richiede, da parte di tutti gli utenti, un codice di identificazione personale (userid) e una parola chiave segreta (password).
Sia nel caso di disattivazione del codice di identificazione personale che nel caso in cui l'utente si dimentichi la propria password, per riottenere l'accesso ai servizi l'utente dovrà compilare nuovamente il modulo per l'utilizzo dei servizi informatici aziendali, allegare la fotocopia di un documento di identità e consegnarlo all'IT firmato che lo consegnerà al responsabile aziendale del trattamento dei dati.

In caso di rinnovo la password può essere consegnata esclusivamente in due modalità:

1. inviata con sms a un cellulare fornito dall'utente;

2. ritirata di persona.

In nessun caso può essere fornita al telefono o inviata con altri mezzi.

La password non potrà essere ceduta a terzi, neppure temporaneamente e dovrà essere mantenuta segreta.
Qualsiasi azione svolta sotto l'autorizzazione offerta dalla coppia userid e password sarà attribuita in termini di responsabilità all'utente titolare del codice user ID, salvo che l'utente dia prova di illecito utilizzo della sua autorizzazione da parte di terzi.
Non sono previsti codici di accesso anonimi.
L'utente deve conservare la password con la massima riservatezza e con la massima diligenza. La password non deve essere banale né contenere riferimenti facilmente riconducibili all'utente.
È modificata da quest'ultimo al primo utilizzo e successivamente almeno ogni volta che lo richieda l'IT.
Il cambio password può essere eseguito agevolmente dall'utente autonomamente.
Dopo sei mesi di non utilizzo dei servizi, o nel caso in cui l'utente perda la qualità che gli consentiva di accedere ai servizi informatici aziendali, la user ID e la password vengono automaticamente disattivati. In quest'ultimo caso, i messaggi di posta elettronica in giacenza vengono eliminati.
L'utente si impegna a comunicare immediatamente all'IT, smarrimento, perdita ovvero appropriazione a qualsivoglia titolo da parte di terzi della password.