ALLEGATO 4

DESCRIZIONE DELLE MISURE
A CONTENIMENTO DEL RISCHIO DI REATO

1. **POTERI**
2. **PROCESSI DECISIONALI**
3. **FLUSSI INFORMATIVI A SCOPO DI CONTROLLO**
4. **REGOLAMENTI E PROTOCOLLI RELATIVI ALLE ATTIVITÀ**
   b) Regolamento per le acquisizioni di beni e servizi ed esecuzioni di lavori in economia
   c) Procedure contabili e fiscali
   d) Procedura omaggi e sponsorizzazioni
   e) Procedura per la protocollazione e la conservazione della documentazione (in corso di definizione)
   f) Regolamento per la selezione del personale destinato all'assunzione o all'instaurazione di rapporti di collaborazione o a progetto
   g) Vademecum dipendenti
   h) Verbalizzazione delle decisioni inerenti l'attività
   i) Regole per l'uso dei sistemi informatici e per la tutela del diritto d'autore e dei segni distintivi
   l) Procedura per i controlli periodici del software installato (in corso di definizione)
   m)Procedura di gestione dei rifiuti
   n) Procedura di due diligence in caso di acquisti di partecipazione in società o partnership
   o) Sistemi di pubblicità e trasparenza
5. **MISURE DI SICUREZZA INFORMATICA**
6. **MISURE DI PREVENZIONE E PROTEZIONE DELLA SICUREZZA E DELLA SALUTE DEI LAVORATORI**
7. **VINCOLI CONTRATTUALI CHE IMPONGONO AGLI OUTSOURCER L'ADOZIONE DI MISURE A CONTENIMENTO DEL RISCHIO DI REATO**

1. POTERI DI RAPPRESENTANZA E VINCOLI DI SPESA

Qui di seguito l'indicazione dei poteri e dei vincoli di spesa

Poteri	Attività
Amministratore Unico	Atti di ordinaria e straordinaria amministrazione, eccetto quelli che per inderogabile disposizione di legge sono riservati alla competente assemblea
	Firma sociale e rappresentanza legale
	Linee generali: Organizzare e sovrintendere alle attività della società vigilando affinché esse si svolgano in conformità alla legge e agli indirizzi impartiti
	Linee gestionali: Condurre operativamente la società nell'ambito e nei limiti dei piani pluriennali e di budget approvati
	Linee organizzative: Dirigere il personale della società per il corretto assolvimento delle funzioni indicate ai punti precedenti.

2. PROCESSI DECISIONALI

Documento di programmazione strategica	
Amministratore Unico	**Assemblea dei Soci**
Indicazione degli obiettivi e dei risultati che si intendono perseguire nel lungo e nel breve periodo	Approvazione del documento sulla base delle indicazioni dei soci

Regolamenti	
Amministratore Unico	**Assemblea dei Soci**
Preventivo vaglio dei regolamenti in materia di: - acquisizione di risorse umane e affidamento di incarichi professionali - definizione ed individuazione della struttura organizzativa degli uffici, sistema di valutazione delle prestazioni individuali ai fini della retribuzione accessoria o degli avanzamenti di carriera; - acquisizione di lavori, forniture e servizi in economia	Approvazione dei regolamenti

Bilancio	
Amministratore Unico	**Assemblea dei Soci**
Assenso alla proposta di bilancio da trasmettersi almeno 30 giorni della data prevista per l'approvazione dell'Assemblea	Approvazione bilancio

3. FLUSSI INFORMATIVI A SCOPO DI CONTROLLO

Flussi informativi da CTC alla Camera di Commercio

- delibere dell'Amministratore Unico e verbali delle Assemblee
- bilanci annuali e suoi successivi aggiornamenti
- politiche di investimento
- politiche di acquisto di beni e servizi e attività contrattuale

4. REGOLAMENTI E PROTOCOLLI RELATIVI ALLE ATTIVITA'

a) PROCEDURE CONTABILI E FISCALI

Emissione fatture

Fatture relative a servizi

Area Amministrativa
A servizio ultimato emette la fattura allegando i documenti che attestano le prestazioni eseguite e i contratti di riferimento.
Registrazione dell'incasso nel programma di contabilità
Revisore Unico
Controllo trimestrale a campione

Liquidazione Iva mensile

Entro il 16 del mese successivo

Area Amministrativa
Stampa dei registri iva (acquisti, vendite, autofatture)
Verifica delle battute (calcolo con calcolatrice dell'imposta evidenziata in fattura) con i totali dei registri iva
Giroconti dei saldi dei partitari (iva c/acquisti, iva c/vendite) e verifica correttezza giroconti (il saldo dei partitari deve essere uguale a zero l'ultimo giorno del mese
Calcolo "a mano" del debito e credito considerando il credito del mese precedente e incrocio dei dati con il saldo Erario c/iva
In caso di debito, autorizzazione al pagamento dell'AU
Area Amministrativa
Invio telematico tramite home banking
Stampa quietanza

Ritenute d'acconto sui compensi

Mensilmente

Area Amministrativa
Viene creata una cartellina cartacea contenente: - copia fattura/proforma/notula - copia bonifico - stampa partitario della banca con evidenziato il pagamento - stampa partitario "Erario c/ritenute" per il debito mensile - copia quietanza di pagamento F24
Entro il 16 del mese si verifica l'eventuale debito all'Erario (partitario) con i documenti contenuti nella cartellina corrispondente ai pagamenti del mese precedente

AU Autorizzazione al pagamento
Area Amministrativa
Pagamento F24 tramite home banking
Stampa quietanza di pagamento

Annualmente

Area Amministrativa
Raccolta delle cartelline mensili
Stampa delle certificazioni da inviare ai percipienti compensi soggetti alla ritenuta d'acconto
Verifica della corrispondenza delle certificazioni con le ritenute operate e versate
Invio delle certificazioni entro il 28 febbraio
Invio dei fascicoli mensili al consulente del lavoro per il 770

b) PROCEDURA OMAGGI E SPONSORIZZAZIONI

I dipendenti di Chioggia Terminal Crociere non possono ricevere omaggi se non di modesto valore e allo stesso modo non possono fare omaggi a terzi, qualunque essi siano, se non espressamente approvati dall'AU.

Inviti, viaggi, prestazioni varie
I dipendenti e di Chioggia Terminal Crociere non possono ricevere da terzi inviti a iniziative e/o viaggi e comunque prestazioni varie, a meno che non siano strettamente attinenti all'attività lavorativa e rientrino in eventi promozionali e di pubbliche relazioni.

Sponsorizzazioni
Eventuali sponsorizzazioni di Chioggia Terminal Crociere ad iniziative, sia pubbliche che private, debbono essere autorizzate dall'AU.
L'eventuale sponsorizzazione di iniziative private è subordinata alla verifica dell'affidabilità del partner di cui al successivo articolo.
Eventuali sponsorizzazioni da parte di soggetti pubblici e privati a favore di Chioggia Terminal Crociere debbono essere autorizzate dall'AU.
L'eventuale sponsorizzazione da parte di soggetti privati è subordinata alla verifica dell'affidabilità del partner, di cui al successivo articolo.

1) Verifica di affidabilità del partner

Eventuali sponsorizzazioni sono subordinate alla verifica di affidabilità del partner attraverso l'acquisizione:

- della visura camerale con relativi soci e amministratori;
- della documentazione antimafia;
- di informazioni reperibili sul web.

c) PROCEDURA PER LA PROTOCOLLAZIONE E CONSERVAZIONE DEI DOCUMENTI

1) Scopo

La presente procedura definisce le modalità con cui viene protocollata e conservata la documentazione aziendale.
La procedura regola:

- la protocollazione dei documenti in entrata e in uscita;
- la conservazione dei documenti aziendali.

2) Elenco dei documenti sottoposti alla presente procedura

I documenti soggetti alla presente procedura sono:

1. documentazione in entrata
2. documentazione in uscita
3. scritture contabili
4. contratti con clienti e fornitori
5. documentazione relativa alle procedure di acquisto di beni e servizi
6. documentazione relativa alla gestione del personale (compresi i relativi adempimenti amministrativi)

7. documentazione attestante adempimenti amministrativi

3) Supporti documentali

La documentazione aziendale è conservata su supporto cartaceo o su supporto informatico. In quest'ultimo caso, si adottano le modalità di conservazione prescritte dalla disciplina normativa.

4) Durata della conservazione

La documentazione aziendale è conservata per la durata prescritta dalla legge. In particolare sono conservati per dieci anni tutti i documenti riconducibili alle scritture contabili ai sensi dell'art. 2220 del codice civile (oltre alle scritture contabili, contratti fatture, lettere, telegrammi).

5) Sistema di protocollazione

I documenti in entrata e in uscita sono protocollati manualmente su appositi registri.

6) Conservazione dei documenti su supporto cartaceo

I documenti su supporto cartaceo sono conservati presso gli uffici di riferimento per quanto riguarda le ultime due annualità e presso l'archivio aziendale per le annualità antecedenti fino ad un massimo di 10 anni salvo termini di legge

E' adottato un sistema informatico che consente di organizzare la documentazione per il suo reperimento.

7) Conservazione dei documenti su supporto informatico

I documenti su supporto informatico sono archiviati nelle cartelle di rete aziendale.

8) Consultazione dei documenti

La consultazione dei documenti da parte dei dipendenti aziendali è ammessa per lo svolgimento delle attività aziendali, con i limiti previsti dalla disciplina in materia di protezione dei dati personali.

9) Riservatezza

La documentazione aziendale costituisce informazione riservata.

L'accesso alla documentazione da parte del personale interno è disciplinato dal precedente articolo.

L'accesso alla documentazione da parte di terzi, la sua comunicazione o la sua diffusione sono ammessi solo previa autorizzazione dell'Amministratore Unico.

d) REGOLAMENTO PER LA SELEZIONE DEL PERSONALE DESTINATO ALL'ASSUNZIONE O ALL'INSTAURAZIONE DI RAPPORTI DI COLLABORAZIONE COORDINATA E CONTINUATIVA O A PROGETTO

E' adottato il suddetto regolamento ai sensi della legge 133/08.
Il regolamento è all'allegato a)

e) REGOLE PER L'USO DEI SISTEMI INFORMATICI E PER LA TUTELA DEL DIRITTO D'AUTORE E DEI SEGNI DISTINTIVI

1)Protezione della stazione di lavoro

La stazione di lavoro (pc, laptop, portatitile etc.) affidata all'utente è uno strumento di lavoro. Deve essere custodita con cura evitando ogni possibile forma di danneggiamento.
L'utente deve mettere in atto tutte le precauzioni possibili al fine di evitare accessi indesiderati o non controllati alla propria dotazione di informatica individuale, in particolare deve:

- assicurarsi che la workstation assegnatagli sia dotata di password all'accensione, in caso contrario deve segnalarlo al proprio responsabile
- se durante l'orario di lavoro lascia incustodita la workstation, deve alternativamente:
  - spegnere la workstation
  - bloccarla
  - effettuare il logout della sessione utente
- attivare comunque, ovunque possibile, il salvaschermo (screen-saver automatico con password) entro i 10 minuti di inutilizzo
- al termine della giornata di lavoro spegnere la workstation oppure disconnettersi dalla propria sessione e passare alla modalità di stand-by o di risparmio energetico.

Nel caso in cui l'utente disponga di portatile, è tenuto a:

- proteggerlo con la password secondo le istruzioni fornite;
- non lasciarlo incustodito, specie in ambienti pubblici
- quando non serve, riporlo sotto chiave
- non registrarvi informazioni sensibili o riservate e, qualora non se ne possa fare a meno, crittografarle.

L'utente è responsabile di fornire il proprio contributo al fine di minimizzare la possibilità che i dati personali o riservati contenuti nella propria workstation o trattati tramite la workstation siano esposti a rischi di sicurezza.

2) Conservazione di informazioni critiche su workstation

E' vietato conservare/mantenere esclusivamente sulla propria workstation, quale archivio o sorgente informativa primaria, archivi/database di dati critici per il business aziendale e/o classificabili come 'personali/sensibili/giudiziari', senza segnalarlo al proprio responsabile gerarchico, per le opportune contromisure, esponendoli quindi al rischio di perdita o danneggiamento anche involontario.

3)Dati personali del dipendente e dismissione delle apparecchiature

La registrazione di dati personali non aziendali da parte dei dipendenti su workstation è ammessa, nel rispetto delle politiche di sicurezza, a meno che non comprometta la funzionalità della workstation e previa separazione (cartelle ad hoc facilmente distinguibili da quelle contenente dati aziendali) o cifratura di tali dati.
All'atto della dismissione, riassegnazione e qualora comunque necessario, è opportuno che anche il dipendente proceda alla *cancellazione sicura* dei propri dati personali eventualmente memorizzati sulla workstation in forma intellegibile.

4)Password e regole relative

La password è un elemento fondamentale per la sicurezza delle informazioni. La robustezza delle password è il meccanismo più importante per proteggere i dati; un corretto utilizzo della password è a garanzia degli asset aziendali e dell'utente stesso.
Le regole di seguito elencate sono vincolanti per l'accesso a tutti i sistemi e le workstation.

a) Impostazione, variazione iniziale e periodica delle password

- Le password assegnate per qualsiasi scopo devono essere sostituite al primo utilizzo.
- Tutte le password di default (ad es. “system”, “administrator”) devono essere cambiate al momento dell’installazione del prodotto o del sistema.
- Tutte le password devono essere cambiate almeno ogni 6 mesi a cura degli incaricati (titolari delle credenziali) ovvero ogni 3 mesi nel caso di accesso a dati sensibili ai sensi della normativa in materia di privacy

b) Regole di utilizzo generali

- Le password non devono essere scritte in chiaro
- Le password non devono essere inserite in chiaro in messaggi e-mail o in altre forme di comunicazione elettronica
- Le password non devono essere comunicate a terzi dal titolare.
- Nel caso in cui il titolare sospetti che la sua password sia venuta a conoscenza di terzi deve essere immediatamente cambiata
- E' obbligatorio custodire idoneamente smart-card, token e business-key contenenti certificati di autenticazione e disinserire i predetti dispositivi dal computer prima di lasciarlo incustodito

c) Gestione delle password nei sistemi

La password dell’utente non deve essere registrata in nessun modo nel log delle sessioni e neppure in nessun altro sistema di logging/debugging

d) Caratteristiche obbligatorie delle password

La lunghezza minima della password è di 8 caratteri o comunque il massimo previsto dalla tecnologia o sistema specifico.
Inoltre la password :

- deve contenere almeno un carattere alfabetico ed uno numerico.
- non deve contenere più di due caratteri identici consecutivi.
- non deve essere simile alla password precedente.
- non deve contenere l’user-id come parte della password.
- non deve essere riconducibile ai dati anagrafici dell’incaricato o di suoi familiari

e) Ripristino della password

Il ripristino della password deve essere eseguito mediate apposita procedura, solo a fronte di una positiva identificazione del richiedente.

La nuova password ottenuta dovrà essere cambiata subito dopo a cura del richiedente stesso.

5) Software

I software non correlati allo svolgimento della specifica attività lavorativa e al di fuori degli standard aziendali, non hanno a priori alcun titolo per essere presenti nelle stazioni di lavoro individuali.

La responsabilità relativa all'installazione dei predetti software è pertanto di chi li installa sulla stazione di lavoro, a meno di documentabile specifica autorizzazione aziendale.

L'installazione da parte del dipendente di software non previsto dalla dotazione standard aziendale sulla propria stazione di informatica individuale o non specificamente autorizzata è ammessa, a responsabilità del dipendente stesso, esclusivamente a condizione che tali software:

- siano compatibili con la funzionalità della stazione di lavoro e con l'espletamento delle mansioni lavorative del dipendente
- non siano pericolosi per la sicurezza delle informazioni aziendali
- non siano in contrasto con le normative di legge, con particolare attenzione a:
    - norme in materia di protezione dei dati personali;
    - norme in tema di copyright;
    - norme contro i reati informatici;
    - politiche di sicurezza aziendali.

Il software che venga rilevato/segnalato in contrasto con quanto sopra detto, deve essere immediatamente rimosso a cura del dipendente stesso.

6)Tutela del software

I software debbono essere acquisiti con regolare licenza e devono essere conservate le prove della titolarità della licenza. E' quindi proibito installare software senza licenza. Per licenza si intende ogni tipo di atto che consente l'utilizzo del software quale, a titolo d'esempio: le licenze di tipo proprietario che consentono solo l'uso del software, le licenze freeware che ne consentono l'uso e la distribuzione, le licenze shareware che subordinano l'uso del software a determinate condizioni, le licenze del freesoftware o del software open source che ammettono anche l'accesso e la modifica del codice sorgente.

Considerando le varie tipologie di licenze e la conseguente diversa disciplina dei diritti sul software è necessario che quanto da esse disposto sia conosciuto e se ne dia scrupolosa attuazione.

L'utilizzo di software freeware e shareware è consentito solo nel caso in cui i programmi siano scaricati da fonti sicure. Sono fonti sicure quelle che danno garanzia che:

1. la distribuzione del software avvenga nel rispetto dei relativi diritti;
2. il software distribuito sia esente da codice malevolo (virus, network worms, trojan horses, logic bombs etc.)

L'utilizzo di free software o di software open source è consentito nei limiti e alle condizioni prescritte dalla relativa licenza, con riferimento in particolare ai vincoli previsti nel caso di distribuzione successiva dello stesso software o delle sue modifiche/integrazioni/evoluzioni.

Nel caso in cui lo sviluppo del software sia affidato a terzi, è necessario assicurarsi, anche contrattualmente, che il software eventualmente impiegato per lo sviluppo sia utilizzato legittimamente nel rispetto del diritto d'autore.

7)Tutela di altri materiali protetti dal diritto d'autore e/o dalla disciplina sui marchi e segni distintivi

L'utilizzo di brani, musica, video, fotografie o altro materiale protetto dal diritto d'autore per la realizzazione di filmati promozionali, presentazioni, report etc. è consentito solo con l'autorizzazione del titolare dei diritti e comunque a condizione di aver verificato il regime d'utilizzo di tali opere e averlo rispettato. A questo proposito si suggerisce di utilizzare materiale distribuito con licenza Creative Commons che non escluda l'utilizzo commerciale del materiale.

Salvo il caso di cui al punto precedente, è assolutamente vietato utilizzare gli strumenti aziendali per scaricare materiale protetto dal diritto d'autore.

L'utilizzo di segni distintivi altrui nell'ambito di iniziative congiunte è consentito solo previa autorizzazione scritta del titolare del segno. Senza il consenso del titolare, non è in alcun modo ammesso l'utilizzo di marchi, loghi e segni distintivi altrui per promuovere direttamente o indirettamente (ad esempio attraverso i metatag) le iniziative dell'azienda sul web.

8)Strumenti di controllo

Sono adottati adeguati strumenti di controllo ed effettuati audit interni, anche automatici, in modo tale da verificare che il software o altro materiale protetto dal diritto d'autore (quale video, musica, foto etc) presente sui computer in dotazione possa essere lecitamente utilizzato. E' proibito inabilitare l'uso di tali strumenti di controllo.

9)Utilizzo corretto di Internet e Posta elettronica

L'azienda mette a disposizione dei dipendenti i servizi di posta elettronica e l'accesso alla rete internet. Nell'utilizzare tali strumenti il dipendente è tenuto ad operare secondo correttezza.

- L'utilizzo dei servizi di posta elettronica e di Internet è consentito:
  - solo attraverso le infrastrutture appositamente predisposte dall'azienda.
  - rispettando le normative di legge in generale e quelle riportate in questo documento in particolare, nonché le politiche di sicurezza aziendali.
- Il dipendente e le terze parti che utilizzano servizi di internet e posta aziendale in azienda devono quindi:
  - agire nel rispetto della legge, con particolare riferimento alle norme in materia di reati informatici
  - seguire le regole in materia di utilizzo corretto di internet e posta elettronica conosciute come 'Netiquette' e le raccomandazioni aziendali tese ad evitare comportamenti scorretti.

L'azienda si riserva il diritto di impedire l'accesso ad alcuni siti internet ritenuti pericolosi per motivi di sicurezza e per conformità alla legislazione (prevenzione di reato).

I comportamenti palesemente scorretti da parte di un utente, quali:

- violare la sicurezza di archivi e computer della rete
- violare la privacy di altri utenti della rete, leggendo o intercettando la posta elettronica loro destinata

- compromettere il funzionamento della rete e degli apparecchi che la costituiscono con programmi (virus, trojan, ecc.) costruiti appositamente;

costituiscono dei veri e propri crimini informatici, come tali punibili anche dalla legge.

10)Utilizzo per ragioni personali di Internet e Posta elettronica

Compatibilmente con la propria attività lavorativa, è consentito utilizzare i servizi di posta elettronica o di rete anche per ragioni personali, purchè tale utilizzo:

- avvenga nel rispetto della legge
- sia senza fini di lucro personale
- non violi alcuna regola di sicurezza aziendale

Va comunque tenuto presente che l'azienda non può garantire a priori la riservatezza di comunicazioni personali e che il dipendente può trovarsi a dover rispondere dell'utilizzo, se scorretto, delle risorse messe a disposizione dall'azienda per fini di lavoro.

E' comunque vietato ai singoli dipendenti l'uso, per motivi personali, di servizi a pagamento che prevedano una fatturazione nei confronti dell'Azienda, salvo esplicita autorizzazione della Direzione.

11)Registrazioni di sicurezza

I sistemi informatici aziendali sono soggetti a registrazioni di sicurezza, in base alle esigenze aziendali, alle politiche di sicurezza in vigore ed in conformità alle disposizioni di legge.

Per garantire la manutenzione della sicurezza e della rete, le funzioni aziendali competenti effettuano controlli anche saltuari od occasionali sugli apparati, sui sistemi e sul traffico in rete.

Il fine di tale attività è comunque la rilevazione di possibili anomalie di utilizzo e la fornitura di un adeguato livello di servizio e non il controllo delle attività dei singoli dipendenti.

f) PROCEDURA DI GESTIONE DEI RIFIUTI

La presente procedura descrive le modalità di gestione dei rifiuti prodotti da Chioggia Terminal Crociere Srl per garantire che essa avvenga nel pieno rispetto delle norme a tutela dell'ambiente.

1) Tipi di rifiuti

Chioggia Terminal Crociere Srl produce i rifiuti tipici dell'attività d'ufficio.

I rifiuti prodotti da Chioggia Terminal Crociere Srl appartengono alle seguenti categorie:

- 160213 apparecchiature fuori uso, contenenti componenti pericolosi, diverso da quelli di cui alle voci 160209 (trasformatori e condensatori contenenti PCB) e 160212 (apparecchiature fuori uso contenenti amianto in fibre libere)
- 160214 apparecchiature fuori uso, diverse da quelle di cui alle voci da 160209 a 160213
- 150101 imballaggi in carta e cartone
- 080318 toner per stampa esauriti, diversi da quelli di cui alla voce 080317 (toner contenenti sostanze pericolose)

2) Raccolta e smaltimento
I rifiuti sono raccolti e smaltiti con le modalità indicate nella tabella che segue.

Tipo di rifiuto	Gestore
• 160213 apparecchiature fuori uso, contenenti componenti pericolosi, diverso da quelli di cui alle voci 160209 e 160212 • 160214 apparecchiature fuori uso, diverse da quelle di cui alle voci da 160209 a 160213 • 080318 toner per stampa esauriti, diversi da quelli di cui alla voce 080317	I rifiuti sono ritirati dalla Camera di Commercio di Venezia Rovigo Delta lagunare nell'ambito del servizio di gestione e manutenzione dell'hardware, di stampanti e fotocopiatrici
• 150101 imballaggi in carta e cartone	I rifiuti sono gestiti dall'impresa di pulizia che li conferisce negli appositi contenitori

3) Interventi specifici
Gli interventi specifici per lo smaltimento dei rifiuti relativi agli interventi di manutenzione straordinaria sono assegnati al fornitore che si occupa dell'attività. I contratti con fornitori definiscono puntualmente gli oneri (operativi ed amministrativi) in capo a questi ultimi.
L'area tecnica si adopera perché il fornitore trasmetta al più presto i certificati di smaltimento prodotti dagli Smaltitori e archivia tali certificati in modo che siano facilmente rinvenibili.

g) SISTEMI DI PUBBLICITA' E TRASPARENZA PREVISTI DALLA NORMATIVA

L'articolo 1 commi da 15 a 33 della legge 190/12 prevede i seguenti obblighi di pubblicità a cui Chioggia Terminal Crociere Srl dà attuazione mediante pubblicazione sulle pagine web dedicate del sito della Camera di Commercio di Venezia Rovigo.

Informazioni da pubblicare ai sensi della legge 190/12	Informazioni che Chioggia Terminal Crociere Srl provvede a pubblicare
Informazioni relative ai procedimenti amministrativi	**Si pubblicano e si mantengono aggiornati i seguenti documenti:** **-Regolamento per la selezione del personale destinato all'assunzione o all'instaurazione di rapporti di collaborazione o a progetto**

Bilanci e conti consuntivi	**Si pubblicano annualmente i bilanci della società**
Costi unitari di realizzazione di opere pubbliche e di produzione dei servizi erogati ai cittadini	**Aggiornamento annuale**
Informazioni sui procedimenti autorizzativi e concessori	**Aggiornamento annuale**
Scelta del contraente per l'affidamento di lavori, forniture e servizi: - struttura proponente - oggetto del bando - elenco operatori invitati a presentare offerte - aggiudicatario - importo di aggiudicazione - tempi di completamento dell'opera, servizio o fornitura - importo delle somme liquidate	**Si pubblicano secondo le istruzioni fornite da Avcp, informazioni in merito a:** **- modalità di scelta del contraente** **- oggetto della fornitura o servizio richiesto** **- elenco operatori invitati a presentare offerte** **- aggiudicatario** **- importo di aggiudicazione** **- durata del contratto (per i servizi)** **- importo delle somme liquidate**
Concessioni ed erogazione di sovvenzioni, contributi, sussidi, ausili finanziari, attribuzione di vantaggi economici	**n.a.**
Concorsi e prove selettive per l'assunzione del personale e progressioni di carriera	**Informazioni su procedure selettive**
Risultati del monitoraggio periodico del rispetto dei tempi procedimentali	**Da applicare al procedimento acquisti e selezione del personale**
Almeno un indirizzo di posta elettronica certificata	**Indirizzo Pec**

5. MISURE DI SICUREZZA INFORMATICA

Le misure di sicurezza informatica sono garantite dalla Camera di Commercio di Venezia Rovigo Delta lagunare, per tramite della sua società in house Infocamere s.p.a, che gestisce il sistema informatico e tutti i servizi informatici utilizzati da Chioggia Terminal Crociere Srl. La Camera di Commercio garantisce:

- la fornitura dell'hardware e del software necessario all'attività lavorativa;
- i servizi di posta elettronica e accesso ad internet;
- le misure di sicurezza a protezione della rete, comprese:
    - registrazione dei log di accesso;
    - firewall;
    - assegnazione di livelli di accesso ai sistemi;
    - sistemi di back up;
- le misure di sicurezza a protezione delle stazioni di lavoro, comprese:
    - credenziali di accesso;
    - screen saver;
    - antivirus.

6. MISURE DI PREVENZIONE E PROTEZIONE DELLA SICUREZZA E DELLA SALUTE DEI LAVORATORI

L'azienda ha redatto e aggiorna regolarmente il Documento di Valutazione dei Rischi,

Il ruolo di RSPP è affidato ad una persona esterna, l'ing. Fabrizio Gallian.

7. VINCOLI CONTRATTUALI CHE IMPONGONO AGLI OUTSOURCER L'ADOZIONE DI MISURE A CONTENIMENTO DEL RISCHIO DI REATO

I fornitori di Chioggia Terminal Crociere Srl sottoscrivono la seguente clausola.

Art. (…) MODELLO ORGANIZZATIVO EX D.LGS. 231/01 E CODICE ETICO

1. Il Fornitore dichiara di aver adottato e di applicare il modello organizzativo previsto dal d.lgs. 231/01 in materia di responsabilità amministrativa degli enti.
2. In caso negativo, il Fornitore si impegna, nell'esecuzione delle attività derivanti dal presente accordo, ad osservare le norme contenute nel Codice Etico di Chioggia Terminal Crociere Srl. Il Fornitore con la conclusione dell'accordo dichiara, quindi, di avere preso visione e di accettare il suddetto Codice Etico.
3. La notizia dell'inosservanza da parte del Fornitore di qualsiasi previsione del Codice Etico o della commissione di reati presupposto della responsabilità amministrativa degli enti comporterà la facoltà di Chioggia Terminal Crociere Srl di risolvere il contratto con effetto immediato, ai sensi e per gli effetti di cui all'art. 1456 c.c.

Allegati

Allegato a)
Regolamento per la selezione del personale destinati all'assunzione o all'instaurazione di rapporti di collaborazione coordinata e continuativa o a progetto