Allegato 4
Descrizione delle misure a contenimento del rischio di reato

Indice Misure

1. POTERI E CONTROLLI

La società è stata messa in liquidazione con decisione dell'Assemblea dei soci del 28 luglio 2015.
Al Liquidatore sono stati attribuiti i poteri ordinari.
La società è dotata di Collegio Sindacale e di società di revisione.

2. PROCEDURA PER IL LICENZIAMENTO DEL PERSONALE SOMMINISTRATO

Il procedimento di liquidazione di JobCamere impone il graduale licenziamento del personale in somministrazione nell'assunto, espressamente dichiarato nell'Assemblea del 28 luglio 2015, che i soci, che tuttora utilizzano i servizi della Società, non subiscano alcuna conseguenza sui contratti attualmente esistenti avendo il tempo necessario per individuare soluzioni operative e attivare canali alternativi di mercato con riferimento alle nuove esigenze di personale in somministrazione.

Il processo di licenziamento del personale in somministrazione, deve, quindi, contemperare le esigenze derivanti dal processo di liquidazione che la società ha avviato con la necessità di consentire ai soci di individuare, per il reperimento del personale, soluzioni alternative a quelle della somministrazione da parte di JobCamere.

I criteri che seguono sono fissati in modo da garantire i principi di trasparenza e imparzialità contemperando i suddetti interessi.

1. JobCamere evidenzia al socio utilizzatore la necessità di trovare, per il reperimento del personale, soluzioni alternative a quelle in essere collaborando attivamente alla loro realizzazione
2. I contratti a tempo determinato vengono mantenuti fino alla loro naturale scadenza a meno che il socio utilizzatore dia disdetta del relativo contratto di somministrazione prima della scadenza o ne chieda il rinnovo. In questo caso, JobCamere, compatibilmente con le norme che disciplinano il contratto di lavoro in somministrazione, provvede assecondando le esigenze del socio utilizzatore.
3. I contratti a tempo indeterminato vengono mantenuti fino a quando il socio utilizzatore dia disdetta del relativo contratto di somministrazione.
4. In ogni caso JobCamere, stante il suo stato di liquidazione, evidenzia al socio utilizzatore la necessità di trovare soluzioni alternative a quelle offerte da JobCamere.
5. Nei casi in cui:
    a. il socio utilizzatore dia disdetta al contratto di somministrazione prima della scadenza;
    b. il contratto di somministrazione arrivi a scadenza e non venga

rinnovato;

c. l'Assemblea dei soci fissi un termine oltre il quale i contratti in essere debbano essere disdettati o non siano più rinnovabili o entro il quale debba concludersi il processo di liquidazione della società;

si prospettano le seguenti eventualità che dipendono dalle decisioni assunte dai soci utilizzatori:

- JobCamere cede il contratto ad altra agenzia per il lavoro a cui il socio utilizzatore ha affidato il servizio di somministrazione;
- Il socio utilizzatore assume direttamente il dipendente. In questo caso JobCamere propone al dipendente di presentare le proprie dimissioni prospettando la contestuale assunzione da parte del socio utilizzatore.

6. Nei casi in cui le eventualità di cui al punto precedente non si realizzino, si procede al licenziamento del dipendente con le procedure previste dalla normativa di riferimento.
7. La disdetta o il rinnovo del contratto di somministrazione sono subordinati ai limiti previsti dalla legge per i contratti con i dipendenti somministrati.
8. Tutte le decisioni relative alla seguente procedura sono adottate dal Liquidatore. Eventuali scostamenti dalla procedura sono comunicati preventivamente all'Organismo di Vigilanza che ne darà atto nei propri verbali valutando che siano comunque rispettati i principi di trasparenza e di imparzialità.
9. L'Organismo di Vigilanza effettuerà audit a campione sul regolare rispetto della presente procedura.

3. PROCEDURA PAGAMENTI

La procedura coinvolge ICOutsorcing e Infocamere

Ricevimento della fattura	Icoutsourcing (Ufficio Servizi Generali)
Verifica della fattura rispetto alle previsioni contrattuali e alle disposizioni fiscali	Icoutsourcing (Ufficio Servizi Generali)
Autorizzazione al pagamento previa verifica della correttezza della prestazione per cui la fattura è stata emessa	Liquidatore
Verifica ai sensi dell'art. 48 bis della legge 601/73	Infocamere (Amministrazione)
Predisposizione del mandato di pagamento e trasmissione all'Istituto di credito	Infocamere (Amministrazione)
Autorizzazione ad effettuare il pagamento via homebanking	Liquidatore

4. DICHIARAZIONE SULLA VERIDICITÀ E COMPLETEZZA DELLE INFORMAZIONI DESTINATE ALLE COMUNICAZIONI SOCIALI

La redazione del bilancio è affidata ad Infocamere a cui è attribuito anche il servizio di gestione contabile. Il bilancio è quindi redatto ricorrendo ai dati estratti dal sistema di gestione contabile con le informazioni/valutazioni fornite dal Liquidatore di JobCamere. Qui di seguito la procedura.

Dichiarazione dei dati di bilancio		
Liquidatore di JobCamere	1	Tramette le informazioni alla Direzione Amministrazione e Controllo di Infocamere le informazioni/valutazioni relative a: - accantonamenti per rischi; - svalutazione sui crediti - etc.
	2	Predispone e trasmette alla Direzione Amministrazione e Controllo di Infocamere la dichiarazione di assunzione di responsabilità di cui al seguente punto (a.)
	3	Trattiene copia della dichiarazione di assunzione di responsabilità presso i propri archivi allegata alle informazioni/valutazioni trasmesse
Direttore Amministrazione e Controllo di Infocamere	4	Acquisisce le informazioni/valutazioni trasmesse dal Liquidatore di JobCamere
	5	Redige il bilancio elaborando i dati contabili forniti da JobCamere attraverso il sistema BAAN e le informazioni/valutazioni fornite dal Liquidatore di JobCamere
	6	Predispone e trasmette al Liquidatore di JobCamere la dichiarazione di cui al seguente punto (b.)

a. (per il Direttore Generale di JobCamere)
Dichiaro che per la redazione del bilancio e delle altre comunicazioni sociali ho trasmesso ad Infocamere le seguenti informazioni/valutazioni :
.....
Dichiaro, altresì che posso documentalmente dimostrare la veridicità e completezza di tali informazioni/valutazioni ricorrendo ai seguenti dati in mio possesso:
.....

b. (per il Direttore Amministrazione e Controllo di Infocamere)
Dichiaro che le informazioni utilizzate per la redazione del bilancio e le altre comunicazioni sociali, sono il risultato dell'elaborazione dei dati contabili forniti da JobCamere attraverso il sistema BAN e delle seguenti informazioni/valutazioni fornite per iscritto dal Liquidatore di JobCamere:
.....

5. VERIFICHE MENSILI BUDGET

Il Controllo di gestione di IC trasmette ogni mese al Liquidatore la situazione che descrive gli eventuali scostamenti rispetto al budget. L'analisi viene effettuata congiuntamente tra il Liquidatore e il Controllo di gestione. Le eventuali azioni correttive adottate dal Liquidatore vengono recepite dal Controllo di gestione.

6. PROCEDURA PER LA PROTOCOLLAZIONE E LA CONSERVAZIONE DEI DOCUMENTI

Il servizio di protocollazione è fornito da ICOutsourcing.
E' adottato il Manuale di protocollazione che presenta le seguenti caratteristiche:

Caratteristiche	**Risultati**
Livelli di autorizzazione per consultazione, inserimento, modifica	Abilitati a tutte le funzioni consentite sono solo due persone dell'Ufficio Protocollo. Il Liquidatore e la Responsabile commerciale sono abilitati alla protocollazione in uscita.
Rispetto dei termini per la registrazione di protocollo	La protocollazione delle comunicazioni in entrata avviene in giornata e comunque non oltre le 48 ore dal ricevimento
Presenza segnatura di protocollo sui documenti	Il documento è scansionato e quindi allegato una volta che gli è stato apposto il numero di protocollo. La segnatura di protocollo è indicata a mano .
Registrazioni annullate e registrazioni modificate	Le registrazioni possono essere annullate. In questo caso il documento viene conservato come annullato con indicazione del motivo.
	Le registrazioni possono essere modificate, ad eccezione del numero di protocollo e del documento protocollato.
Richiesta di numerazione di protocollo per e.mail	Le comunicazioni via e.mail, che comportano l'assunzione di impegni, vengono protocollati prima di essere inviati.
Acquisizione immagine dei documenti	Tutti i documenti protocollati sono acquisiti come immagini e quindi sono conservati indicizzati nel sistema
Assegnazione ai destinatari	La posta in arrivo viene smistata secondo i seguenti criteri: - se i destinatari sono il Liquidatore o l'Ufficio Personale di ICO, che gestisce il servizio di gestione del personale, viene recapitata loro direttamente. Saranno loro a richiederne l'eventuale protocollazione; -se i destinatari sono altri o non sono indicati, la posta viene protocollata e quindi smistata.
Archiviazione dei documenti cartacei presso l'ufficio protocollo	I documenti sono archiviati e indicizzati
Trasmissione di fatture, ordini e contratti in originale	L'ufficio protocollo scansiona il documento e trasmette l'originale a Infocamere.

ad Infocamere per la gestione in outsourcing	
Collegamento tra più protocolli	Il numero di protocollo è univoco. Non è attiva la funzione che associa i numeri di protocollo a formare un fascicolo
Attribuzione livello di riservatezza	Viene utilizzata la funzione che indica il documento come riservato. In questo caso è visibile solo alla Responsabile del protocollo di ICO e al Liquidatore

7. PROCEDURA PER L'ATTRIBUZIONE DEL CODICE CIG (CODICE IDENTIFICATIVO GARA)

- Il responsabile dell'acquisto invia alla segreteria copia del preventivo, dell'offerta o del contratto per l'acquisto con i seguenti dati:
  - numero di protocollo,
  - importo totale,
  - oggetto
  - eventuale IBAN
  - data inizio/fine contratto

- Se l'importo è inferiore a 40.000 euro, la segreteria richiede il CIG sul sito dell'AVCP (Autorità di Vigilanza nei Contratti Cubblici) tramite la procedura semplificata (Sistema per il rilascio del CIG in modalità semplificata) che prevede l'inserimento dei seguenti dati:
  - fattispecie contrattuale,
  - importo totale,
  - oggetto
  - procedura di scelta contraente
  - oggetto principale del contratto (lavori, servizi o furniture)

- Se l'importo è tra 40.000 e 150.000 euro, la segreteria utilizza, sempre sul sito dell'AVCP, la procedura standard che richiede l'inserimento di ulteriori informazioni (es. luogo, codice ISTAT)
- Se l'importo supera i 150.000 euro, la segreteria utilizza la procedura standard e compila sul sito la scheda relativa ai dati del fornitore.
- A conclusione della procedura, la segreteria ottiene il CIG che attribuisce al contratto.
- Entro il 20 di ogni mese, la segreteria trasmette all'Amministrazione di Infocamere un file excel con i seguenti dati:
  - Fornitore
  - Protocollo
  - Date contratto (inizio e scadenza della fornitura in caso di canoni e solo inizio fornitura in caso di acquisto di beni o di servizio una-tantum)
  - Oggetto
  - Importo totale
  - Numero CIG

- IBAN del conto corrente dedicato.

8. SISTEMA DI GESTIONE DELLA SICUREZZA SUL LAVORO

Il sistema è descritto a parte.

9. VINCOLI CONTRATTUALI CON L'UTILIZZATORE IN MATERIA DI SICUREZZA SUL LAVORO A PROTEZIONE DEI DIPENDENTI SOMMINISTRATI

Per quanto riguarda la sicurezza dei lavoratori somministrati, nei contratti tra JobCamere e l'utilizzatore si prevede quanto segue:

- L'Utilizzatore. ai sensi dell'art. 23, II periodo del comma 5 del d.lgs. 276/03 si impegna ad informare i prestatori di lavoro somministrati sui rischi per la sicurezza e la salute connesse all'attività produttiva in generale ed a formare ed addestrare loro all'uso delle attrezzature di lavoro necessarie allo svolgimento dell'attività lavorativa per la quale essi vengono assunti, in conformità alle disposizioni contenute nel d.lgs. 81/2008
- L'Utilizzatore, ai sensi dell'art. 21 comma 1, lett. d) del d.lgs. n. 276/03 indica la presenza di rischi per l'integrità e la salute del lavoratore e le misure di prevenzione adottate che si impegna a comunicare al somministratore tramite il modello "All. A – Modello di informazione sui rischi per l'integrità e la salute dei lavoratori e elle misure di prevenzione adottate" – che allegato al presente contratto ne costituisce parte integrante. Tale modulo, ai sensi dell'art. 21 comma 3 verrà consegnato in copia al lavoratore da parte del somministratore all'atto di stipula del contratto di lavoro.

10. MISURE DI SICUREZZA INFORMATICA

I server sono collocati presso la server farm di Infocamere le cui policy, procedure e misure di sicurezza informatica operano come misure a contenimento del rischio di reato.

Lo schema sotto riguarda le misure di sicurezza informatica relative alle stazioni di lavoro (anche portatili) utilizzate dal personale IobCamere per la propria attività presso l'azienda. Per quanto riguarda le stazioni di lavoro utilizzate dal personale somministrato, sono gli Utilizzatori a disporre le misure di sicurezza necessarie e JobCamere non ha poteri/competenze in materia.

Competenze in materia di sicurezza informatica	JobC	IC
Approntamento dell'hardware con credenziali di accesso alla macchina e screen saver		√
Verifica del cambio password e controllo sulla password per l'accesso ai sistemi in rete		√
Assegnazione dei livelli di accesso ai sistemi*	√	√

Acquisizione sofware standard d'ufficio	√	√
Acquisizione sofware specifico	√	
Antivirus		√
Dismissione delle macchine	√	
Sicurezza della rete, di internet, della posta elettronica e dei sistemi su cui JobCamere è chiamata ad operare		√

*I livelli di accesso dei dipendenti sono definiti da JobCamere e trasmessi ad IC che ne da attuazione (dominio per accesso ad ICnet e internet).

11. REGOLE DI COMPORTAMENTO RELATIVE ALL'USO DEI SISTEMI INFORMATICI

1. 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.

2. Protezione della stazione di lavoro

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.

3. Manutenzione di informazioni critiche su workstation

E' vietato conservare/manutenere 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.

4. 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.

5. 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. Suggerimenti per la costruzione di password robuste

Le password devono essere ricordabili facilmente ma devono essere al contempo robuste. Un modo per ottenere ciò è costruire password che si basino sul titolo di una canzone, su di una frase storica o su di una poesia e assemblarne i pezzi.

Ad esempio, la poesia potrebbe essere: "Mi illumino di immenso" ed una password ricavabile da quella poesia potrebbe essere costruita prendendo le prime due lettere di ogni parola con la prima in carattere maiuscolo ottenendo: "MiIlDiIm".

Da "Quel mazzolin di fiori" si può ottenere: "QuMaDiFi".

Per inserire anche caratteri numerici si può sostituire le "i" con il numero "1" o le "o" con lo zero.

Nel seguito sono descritte le caratteristiche delle password robuste e le caratteristiche delle password deboli.

- Password robuste

Una password intrinsecamente robusta ha le seguenti caratteristiche:

- Contiene sia caratteri maiuscoli sia caratteri minuscoli
- Contiene cifre, lettere maiscole e minuscole e altri caratteri ammessi dal sistema in uso
- E' lunga più di otto caratteri
- Non è una parola di una qualunque lingua, dialetto o linguaggio specialistico
- Non si basa su informazioni personali

-Password deboli

Una password intrinsecamente debole ha una o più delle seguenti caratteristiche:

- è una parola che si trova sul vocabolario
- è una parola di uso comune come, ad esempio: nomi propri, cognomi, personaggi di fantasia (es. Mario, Rossi, Pluto, …)
- è il nome dell'ente o dell'azienda
- è una data di nascita, un indirizzo, un numero di telefono, una targa automobilistica
- è una sequenza banale di caratteri come, ad esempio: aaabbb, qwerty, 123456
- è una qualsiasi password precedentemente menzionata scritta a rovescio
- è una qualsiasi password precedentemente menzionata preceduta o seguita da una cifra

  L'aggiunta di cifre prima o dopo una password debole non modifica la sua debolezza (es. Mario99 o 99Mario sono password deboli).

f. Framework di supporto

Dove la tecnologia lo permette tali regole sono rese obbligatorie dal software altrimenti è responsabilità dell'utente rispettarle.

g. 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.

6. 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.

7. Tutela del diritto d'autore

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:

- la distribuzione del software avvenga nel rispetto dei relativi diritti;
- 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.

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 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.

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.

8. 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.

9. 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.

10. 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.

12. ISTRUZIONI PER L'IMPIEGO DI CITTADINI DI PAESI TERZI

Il servizio è fornito da ICOutsourcing che si attiene alle seguenti regole:

- Nel caso di impiego di cittadini di paesi terzi tra la documentazione richiesta ai sensi dell'articolo 6 Offerta di impiego del Regolamento per la ricerca, la selezione e la gestione del personale, vi è quella che attesta l'eventuale permesso di soggiorno;
- Nel database di gestione del personale si tiene memoria della scadenza del permesso di soggiorno in modo da potere sollecitare la presentazione della documentazione che attesta il rinnovo o della richiesta nei termini di legge dello stesso.

13. PROCEDURE OUTSOURCER

Qui di seguito sono citate le procedure che disciplinano l'attività svolta dagli outsourcer nell'erogazione dei servizi a favore di JobCamere.

A. **REGOLAMENTO DI ICOUTSOURCING PER L'ACQUISIZIONE DI FORNITURE E SERVIZI IN ECONOMIA**
B. **PROCEDURA DI ICOUTSOURCING PER LA GESTIONE DEL RAPPORTO DI LAVORO**
C. **TRAVEL POLICY DI ICOUTSOURCING**
D. **PROCEDURA DI ICOUTSOURCING PER LA GESTIONE DEI RIFIUTI**
E. **PROCEDURA DI INFOCAMERE PER L'ADEMPIMENTO DEGLI OBBLIGHI CONTABILI, AMMINISTRATIVI E FISCALI**
F. **POLICY, PROCEDURE E MISURE DI SICUREZZA INFORMATICA DI INFOCAMERE**

L’ attività svolta dal personale somministrato è disciplinato dalle procedure e policy dell’azienda o dell’ente presso cui quest’ultimo è collocato (ad esempio le procedure di Infocamere di gestione delle banche dati e servizi, le procedure per l’erogazione dei servizi di Certification Authority o le procedure delle Camere di Commercio che disciplinano il lavoro svolto dagli uffici presso cui è collocato il personale somministrato). JobCamere non è in grado di verificare il rispetto di tali procedure né tanto meno la loro efficacia. Ai fini del presente modello sono comunque considerati strumenti a contenimento del rischio di reato anche se il controllo sulla loro attuazione non è presidiato da JobCamere.