

**MODELLO DI ORGANIZZAZIONE,
GESTIONE E CONTROLLO AI SENSI
DEL D.LGS 231/2001**

ALLEGATO B

**Delitti informatici e trattamento
illecito di dati
(art. 24 – *bis* D.lgs. 231/01)**

CASA DI CURA PRIVATA CITTÀ' DI BRA
Via Montenero n. 1
Bra 12042 (CN)

INDICE

B1_ Reati di cui all'art. 24 - *bis* del D.lgs. 231/01

B2_ Aree a rischio

B3_ Principi generali di comportamento

B1_ Reati di cui all'art. 24 – bis del D.lgs. 231/01. Possibili modalità di commissione

Si riporta, qui di seguito, l'elenco dei reati richiamati dall'art. 24 - bis del D.lgs. 231/01 che la Società ritiene potenzialmente applicabili nell'ambito della conduzione delle attività aziendali.

Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491 – bis c.p.)

“Se alcuna delle falsità previste dal presente capo (capo III “Della falsità in atti”) riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti gli atti pubblici”.

In relazione alla commissione del reato di cui all'art. 615 – ter c.p. si applica all'ente la sanzione pecuniaria sino a 400 quote.

Accesso abusivo ad un sistema informatico o telematico (art. 615 – ter c.p.)

“Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

La pena è della reclusione da due a dieci anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa minaccia o violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento ovvero la sottrazione, anche mediante riproduzione o trasmissione o l'inaccessibilità al titolare dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da tre a dieci anni e da quattro a dodici anni”.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

Si parla di danneggiamento informatico quando, considerando sia la componente hardware che quella software, anche separatamente, interviene una modifica tale da impedirne il funzionamento, anche solo parziale.

Per quanto concerne l'accesso abusivo ad un sistema informatico o telematico, la legislazione vuole punire tale condotta anche quando non ne consegua un vero e proprio danneggiamento. Tecnicamente, tuttavia, è improbabile che l'accesso possa avvenire

senza la rimozione di sicurezze, alterazione di password ovvero altro genere di forzatura del sistema, che l'art. 615 c.p. considera siano presenti a protezione del sistema stesso.

In relazione alla commissione del reato di cui all'art. 615 – *ter* c.p. si applica all'ente la sanzione pecuniaria da 200 a 700 quote. In caso di condanna, si applicano altresì le sanzioni interdittive previste dall'art. 9, co. 2, lett. a),b) ed e) del D.lgs. 231/01.

Detenzione, diffusione ed installazione abusiva di codici e di altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615 – *quater* c.p.)

*“Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, abusivamente si procura, detiene, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione fino a due anni e con la multa fino ad Euro 5.164. La pena è della reclusione da due anni a sei anni quando ricorre taluna delle circostanze di cui all'art. 615-ter, secondo comma, n. 1). La pena è della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'art. 615 – *ter*, terzo comma”.*

In relazione alla commissione del reato di cui all'art. 615 – *quater* c.p. si applica all'ente la sanzione pecuniaria sino a 400 quote.

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 - *quater* c.p.)

“Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da un anno sei mesi a cinque anni.

Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa. Tuttavia si procede d'ufficio e la pena è della reclusione da quattro a dieci anni se il fatto è commesso:

- 1) in danno di taluno dei sistemi informatici o telematici indicati nell'art. 615- *ter*, terzo comma;*
- 2) in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni o da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema.*

In relazione alla commissione del reato di cui all'art. 617 – *quater* c.p. si applica all'ente la sanzione pecuniaria da 200 a 700 quote. In caso di condanna, si applicano altresì le sanzioni interdittive previste dall'art. 9, co. 2, lett. a),b) ed e) del D.lgs. 231/01.

Detenzione, diffusione ed installazione abusiva di apparecchiature e di altri mezzi atti ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 - *quinquies* c.p.)

“Chiunque, fuori dai casi consentiti dalla legge, al fine di intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o di interromperle, si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparecchiature, programmi, codici, parole chiave o altri mezzi atti ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.

Quando ricorre taluna delle circostanze di cui all'art. 617 – quater, quarto comma, numero 2), la pena è della reclusione da due a sei anni.

Quando ricorre taluna delle circostanze di cui all'art. 617 – quater, quarto comma, numero 1), la pena è della reclusione da tre a otto anni.

In relazione alla commissione del reato di cui all'art. 617 – *quinquies* c.p., si applica all'ente la sanzione pecuniaria da 200 a 700 quote. In caso di condanna, si applicano altresì le sanzioni interdittive previste dall'art. 9, co. 2, lett. a),b) ed e) del D.lgs. 231/01.

Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.)

“Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da due a sei anni.

La pena è della reclusione da tre a otto anni:

- *se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso di qualità di operatore del sistema;*
- *se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato.*

In relazione alla commissione del reato di cui all'art. 635 – *bis* c.p., si applica all'ente la sanzione pecuniaria da 200 a 700 quote. In caso di condanna, si applicano altresì le sanzioni interdittive previste dall'art. 9, co. 2, lett. a),b) ed e) del D.lgs. 231/01.

Danneggiamento di sistemi informatici o telematici (art. 635 - *quater* c.p.)

“Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635 - bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da due a sei anni.

La pena è della reclusione da tre a otto anni:

- *se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso di qualità di operatore del sistema;*
- *se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato.*

In relazione alla commissione del reato di cui all'art. 635 – *quater* c.p., si applica all'ente la sanzione pecuniaria da 200 a 700 quote. In caso di condanna, si applicano altresì le sanzioni interdittive previste dall'art. 9, co. 2, lett. a),b) ed e) del D.lgs. 231/01.

Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 635 – *quater*.1 c.p.)

Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico ovvero le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici è punito con la reclusione fino a due anni e con la multa fino a euro 10.329.

La pena è della reclusione da due a sei anni quando ricorre taluna delle circostanze di cui all'art. 615 – *ter* c.p., secondo comma, numero 1).

La pena è della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'art. 615 – *ter*, terzo comma.

In relazione alla commissione del reato di cui all'art. 635 – *quater* c.p., si applica all'ente la sanzione pecuniaria sino a 400 quote.

Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 – *quinquies* c.p.)

Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032.

In relazione alla commissione del reato di cui all'art. 640 – *quinquies* c.p., si applica all'ente la sanzione pecuniaria sino a 400 quote.

Estorsione informatica (art. 629, co. 3 c.p.)

Chiunque, mediante le condotte di cui agli artt. 615 – *ter*, 617 – *quater*, 617 – *sexies*, 635 – *bis*, 635 – *quater* e 635 – *quinquies* ovvero con la minaccia di compierle, costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei a dodici anni e con la multa da euro 5.000 ad euro 10.000. La pena è della reclusione da otto a ventidue anni e della multa da euro 6.000 ad euro 18.000, se concorre taluna delle circostanze indicate nel terzo comma dell'art. 628 nonché nel caso in cui il fatto sia commesso nei confronti di persona incapace per età o per infermità.

In relazione alla commissione del reato di cui all'art. 629 co. 3 c.p., si applica all'ente la sanzione pecuniaria da 300 a 800 quote. In caso di condanna, si applicano altresì le sanzioni interdittive previste dall'art. 9 co.2 del D.lgs. 231/01 per una durata non inferiore a due anni.

B2_ Aree a rischio

L'attività di risk assessment ha consentito di individuare nell'ambito della struttura organizzativa di CCBRA, delle aree considerate a rischio, ovvero dei settori e/o dei processi aziendali rispetto ai quali è stato ritenuto astrattamente sussistente il rischio di commissione dei reati sopra richiamati.

Nell'ambito di ciascuna area a rischio sono state individuate le attività sensibili e i protocolli specifici di comportamento e di controllo.

Area a rischio n. 1 Gestione dei sistemi informatici

- Installazione/mantenimento apparati informatici (software/hardware)
- Monitoraggio accessi ai sistemi informatici/telematici
- Accesso a sistemi informatici/telematici esterni
- Gestione della documentazione in formato digitale

Protocolli specifici di comportamento e di controllo

Nell'espletamento delle rispettive attività/funzioni le risorse coinvolte nella presente area sono tenute al rispetto delle seguenti procedure interne: "Norme generali sull'uso della posta elettronica, sulla navigazione in internet e la trasmissione dati" e "Norme generali sullo delle postazioni di lavoro e per la gestione delle password", nonché al rispetto delle misure di sicurezza indicate nel Registro delle attività di trattamento ex art. 30 del Reg. UE n. 679/16. Inoltre, sono previsti i seguenti protocolli specifici di comportamento e di controllo:

- fornire, ai destinatari, un'adeguata informazione relativamente al corretto utilizzo delle risorse informatiche aziendali e al rischio della commissione di reati informatici;
- limitare l'accesso attraverso risorse aziendali a reti e sistemi informatici esterni alla società compatibilmente con le necessità lavorative;
- effettuare controlli periodici sulla rete informatica aziendale al fine di individuare comportamenti anomali quali, a titolo di esempio, il *download* di *files* di grosse dimensioni, ovvero attività eccezionali dei *servers* al di fuori degli orari di operatività sociale;
- predisporre e mantenere adeguate difese fisiche a protezione dei *servers* della Società e più in generale a protezione di ogni sistema informatico societario anche attraverso la predisposizione di un sistema di controllo degli accessi alle sale *servers* prevedendo, ove possibile, controlli per prevenire l'ingresso e l'uscita di materiale non autorizzato;
- informare adeguatamente gli utilizzatori di sistemi informatici dell'importanza di mantenere i propri codici di accesso (*username* e *password*) confidenziali e di non divulgare gli stessi a soggetti terzi;

- diffondere agli utilizzatori di sistemi informatici uno specifico documento con il quale gli stessi si impegnino al corretto utilizzo delle risorse informatiche aziendali;
- informare gli utilizzatori di sistemi informatici della necessità di non lasciare incustoditi i propri sistemi informatici e della convenienza di bloccarli, qualora si dovessero allontanare dalla postazione di lavoro, con i propri codici di accesso;
- impostare i sistemi informatici stessi in modo tale che, qualora non vengano utilizzati per un determinato periodo di tempo, si blocchino automaticamente;
- l'accesso da e verso l'esterno (connessione alla rete Internet) deve essere autorizzato e deve essere effettuato solo con le modalità consentite ed ai fini di utilizzo per scopi lavorativi;
- dotare la stanza *servers* di porta con un controllo di accesso fisico consentito solo a personale autorizzato;
- proteggere ogni sistema informatico societario, al fine di prevenire l'illecita installazione di dispositivi *hardware* in grado di intercettare le comunicazioni relative ad un sistema informatico o telematico, o intercorrenti tra più sistemi, ovvero capace di impedirle o interromperle;
- fornire ogni sistema informatico di adeguato *software firewall* e antivirus e far sì che, ove possibile, questi non possano venir disattivati;
- vietare l'installazione e l'utilizzo di *software* (programmi) non approvati dalla Società e non correlati con l'attività professionale espletata da parte dei destinatari o degli utilizzatori;
- limitare l'accesso alle aree e ai siti Internet particolarmente sensibili poiché veicolo per la distribuzione e diffusione di programmi infetti (c.d. "virus") capaci di danneggiare o distruggere sistemi informatici o dati in questi contenuti (ad esempio, siti di posta elettronica o siti di diffusione di informazioni e *files*);
- vietare, in particolare, l'installazione e l'utilizzo, sui sistemi informatici della Società, di *software* (c.d. "P2P", di *files sharing* o di *istant messaging* non autorizzati) mediante i quali è possibile scambiare con altri soggetti all'interno della rete Internet ogni tipologia di *files* (quali filmati, documenti, canzoni, virus, etc.) senza alcuna possibilità di controllo da parte della Società;
- proteggere i collegamenti *wireless* (ossia senza fili, mediante *routers* dotati di antenna WiFi), eventualmente utilizzati per la connessione alla rete, impostando una chiave d'accesso, onde impedire che soggetti terzi, esterni alla Società, possano illecitamente collegarsi alla rete Internet tramite i *routers* della stessa e compiere illeciti ascrivibili ai dipendenti della Società;
- prevedere un procedimento di autenticazione mediante *username* e *password* al quale corrisponda un profilo limitato della gestione di risorse di sistema, specifico per ogni destinatario o categoria di destinatari;
- i codici identificativi (user-id) per l'accesso alle applicazioni ed alla rete siano individuali ed univoci;
- la corretta gestione delle password sia definita da linee guida, comunicate a tutti gli utenti, per la selezione e l'utilizzo della parola chiave;
- siano definiti i criteri e le modalità per la creazione delle password di accesso alla rete, alle applicazioni, al patrimonio informativo aziendale e ai sistemi critici o sensibili (ad es. lunghezza minima della password, regole di complessità, scadenza);
- gli accessi effettuati dagli utenti, in qualsiasi modalità, ai dati, ai sistemi ed alla rete siano oggetto di verifiche periodiche;
- le applicazioni tengano traccia delle modifiche ai dati compiute dagli utenti;
- siano definiti i criteri e le modalità per l'assegnazione, la modifica e la cancellazione dei profili utente;

- in caso di mancato utilizzo delle credenziali per un periodo pari al almeno 6 mesi, di perdita delle stesse o di cessazione dal rapporto di lavoro con la Società, i responsabili dei sistemi informatici debbono procedere immediatamente alla disattivazione delle stesse, con il supporto dell'amministratore di sistema (se nominato);
- sia predisposta una matrice autorizzativa - applicazioni/profilo/richiedente - allineata con i ruoli organizzativi in essere e coerente con i principi di segregazione dei principi di segregazione dei ruoli;
- siano eseguite verifiche periodiche dei profili utente al fine di verificare che siano coerenti con le responsabilità assegnate e coerente con i principi di segregazione dei principi di segregazione dei ruoli;
- l'accesso alle informazioni che risiedono sui server e sulle banche dati aziendali, è limitato da idonei strumenti di autenticazione tra cui a titolo esemplificativo e non esaustivo: 1) utilizzo di account e password; 2) accessi profilati alle cartelle di rete;
- una verifica delle credenziali utente è effettuata periodicamente al fine di prevenire eventuali erronee abilitazioni ai sistemi applicativi;
- l'attivazione o la modifica di un profilo utente è autorizzata da parte del Responsabile del Servizio informativo ed informatico;
- la documentazione riguardante ogni singola attività sia archiviata allo scopo di garantire la completa tracciabilità della stessa;
- I delitti di criminalità informatica includono anche i c.d. reati di falso. E' pertanto assolutamente vietata la trasmissione di qualsiasi atto non veritiero, contraffatto o non autentico attraverso un invio telematico.

Con riferimento alla gestione delle infrastrutture:

- siano definiti i criteri e le modalità per la gestione dei sistemi hardware che prevedano la compilazione e la manutenzione di un inventario aggiornato dell'hardware in uso presso la Società e che regolamentino le responsabilità e le modalità operative in caso di implementazione e/o manutenzione di hardware;
- siano definiti i criteri e le modalità per le attività di back up che prevedano, per ogni applicazione hardware, la frequenza dell'attività, le modalità, il numero di copie ed il periodo di conservazione dei dati;
- siano definiti i criteri e le modalità per la gestione dei sistemi software che prevedano la compilazione e manutenzione di un inventario aggiornato del software in uso presso la società, l'utilizzo di software formalmente autorizzato e certificato e l'effettuazione di verifiche periodiche sui software installati e sulle memorie di massa dei sistemi in uso al fine di controllare la presenza di software proibiti e/o potenzialmente nocivi;
- siano definiti un piano di business continuity ed uno di disaster recovery periodicamente aggiornati e testati;
- siano definiti i criteri e le modalità per il change management (inteso come aggiornamento o implementazione di nuovi sistemi/servizi tecnologici);
- siano definite le credenziali fisiche di accesso ai siti ove risiedono i sistemi informativi e le infrastrutture IT quali, a titolo esemplificativo, codici di accesso, token authenticator, pin, badge, e la tracciabilità degli stessi;
- siano definite le misure di sicurezza adottate, le modalità di vigilanza e la relativa frequenza, la responsabilità, il processo di reporting delle violazioni/effrazioni dei locali tecnici o delle misure di sicurezza, le contromisure da attivare;
- la documentazione riguardante ogni singola attività sia archiviata allo scopo di garantire la completa tracciabilità della stessa;
- la rete di trasmissione dati aziendale è protetta da adeguati strumenti di limitazione degli accessi (firewall e proxy);

- la rete di trasmissione dati aziendale è segmentata al fine di limitare la possibilità di intercettazioni;
- la rete di trasmissione dati aziendale è protetta da adeguati strumenti di monitoraggio contro il rischio di accesso abusivo;
- i server e le workstation della Società (postazioni fisse e portatili) sono protetti contro potenziali attacchi esterni attraverso l'utilizzo di software antivirus, che effettua controlli in entrata e in uscita, costantemente aggiornati;
- esecuzione di attività di monitoraggio sugli apparati di rete;
- l'accesso ad internet è regolamentato e filtrato da un sistema di web filtering;
- l'attività di navigazione su internet è tracciata;
- assicurare che presso le postazioni di lavoro individuali e presso i server siano installati esclusivamente software originali, debitamente autorizzati o licenziati, e che sia rispettato il limite di installazioni / utenze consentito dalle relative licenze;
- assicurare che l'accesso a database di terzi, di cui si sia acquisito regolare diritto, sia consentito in modo ristretto agli utenti che ne hanno necessità in base alle mansioni svolte.

Le procedure interne “Norme generali sull'uso della posta elettronica, sulla navigazione in internet e la trasmissione dati” e “Norme generali sullo delle postazioni di lavoro e per la gestione delle password” ed il Registro delle attività di trattamento ex art. 30 del Gdpr sono consultabili al seguente link:

[REG. UE n. 679/2016 GDPR REGOLAMENTO EUROPEO GENERALE SULLA PROTEZIONE DEI DATI | Documentazione online | Casa di cura Città di Bra](#)

Area a rischio n. 2 Compilazione, gestione e verifica delle cartelle cliniche e ambulatoriali, delle schede di dimissioni ospedaliere

Nell'espletamento delle rispettive attività le risorse coinvolte nella presente area a rischio sono tenute al rispetto delle seguenti procedure/istruzioni operative di cui al Manuale di Qualità ed in particolare: “La compilazione cartella clinica” (I 11), “Gestione della documentazione sanitaria” (All.1/Sez. 7.5), “Compilazione, invio flusso e controllo della documentazione sanitaria” (All. 11/Sez. 5.4).

Le procedure in oggetto sono consultabili al seguente link:

[Manuale della qualità | Documentazione online | Casa di cura Città di Bra](#)

B.3. I principi generali di comportamento

Con riferimento ai reati menzionati al paragrafo B.1, coerentemente con i principi del Codice Etico, è espressamente vietato:

- utilizzare le risorse informatiche (es. *personal computer* fissi o portatili) assegnate per finalità diverse da quelle lavorative;
- porre in essere condotte, anche con l'ausilio di soggetti terzi, miranti all'accesso a sistemi informativi altrui con l'obiettivo di:
 - acquisire abusivamente informazioni contenute nei suddetti sistemi informativi;
 - danneggiare, distruggere dati contenuti nei suddetti sistemi informativi;

- utilizzare abusivamente codici d'accesso a sistemi informatici e telematici nonché procedere alla diffusione degli stessi;
- distruggere o alterare documenti informatici archiviati sulle *directory* di rete o sugli applicativi aziendali se non espressamente autorizzati, e in particolare i documenti che potrebbero avere rilevanza probatoria in ambito giudiziario;
- utilizzare o installare programmi diversi da quelli autorizzati dalla Responsabile del Servizio informativo ed informatico;
- accedere ad aree riservate (quali server rooms, locali tecnici, ecc.) senza idonea autorizzazione, temporanea o permanente;
- aggirare o tentare di aggirare i meccanismi di sicurezza aziendali (*antivirus*, *firewall*, *proxy server*, ecc.);
- lasciare il proprio personal computer sbloccato e incustodito;
- rivelare ad alcuno le proprie credenziali di autenticazione (nome utente e *password*) alla rete aziendale o anche ad altri siti/sistemi;
- detenere o diffondere abusivamente codici di accesso a sistemi informatici o telematici di terzi o di enti pubblici;
- intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche;
- utilizzare in modo improprio gli strumenti di firma digitale assegnati;
- alterare in qualsiasi modo il funzionamento di un sistema informatico o telematico della Pubblica Amministrazione, o intervenire senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico della Pubblica Amministrazione, al fine di procurare un vantaggio alla Società;
- entrare nella rete aziendale e nei programmi con un codice d'identificazione utente diverso da quello assegnato;
- installare, duplicare o diffondere a terzi programmi (*software*) senza essere in possesso di idonea licenza o in supero dei diritti consentiti dalla licenza acquistata (es. numero massimo di installazioni o di utenze).