MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

CONCESSIONI AUTOSTRADALI LOMBARDE S.p.A.

PARTE SPECIALE E

Reati in materia di Delitti informatici e Trattamento illecito dei dati

ai sensi del Decreto Legislativo 8 giugno 2001, n. 231

INDICE

La presente Sezione costituisce parte integrante del Modello di Organizzazione, Gestione e Controllo di cui Concessioni Autostradali Lombarde S.p.A. si è dotata al fine di soddisfare le esigenze preventive di cui al D.Lgs. 231/01.

Tutti i destinatari del Modello, così come individuati nella parte generale del medesimo, sono chiamati all'osservanza dei principi e delle linee di condotta di seguito indicati, nonché ad adottare, ciascuno in relazione alla funzione in concreto esercitata, comportamenti conformi ad ogni altra norma e/o procedura che regoli in qualsiasi modo attività rientranti nell'ambito di applicazione del Decreto.

1. Premessa

L'art. 7 della legge 18 marzo 2008 n. 48, mediante l'inserimento nell'ambito del D. Lgs. 231/01 dell'art 24 bis sui delitti informatici e trattamento illecito dei dati di seguito riportati, ha introdotto nuove fattispecie di reato che possono generare una responsabilità in capo alla Società.

L'adozione da parte di Concessioni Autostradali Lombarde S.p.A. di un sistema di organizzazione e controllo ai sensi del D. Lgs. 231/01 in grado di prevenire adeguatamente le differenti ipotesi di illecito introdotte con tale normativa, trova il proprio presupposto fondamentale nella volontà, già chiaramente espressa dalla Società, di gestire la propria rete informatica attraverso l'adozione di regole e procedure alla cui osservanza tutti i propri dipendenti sono chiamati.

A tale scopo Concessioni Autostradali Lombarde S.p.A. si avvale di un soggetto qualificato, con lo specifico incarico di gestire i sistemi informatici della rete, anche attraverso un costante monitoraggio avente ad oggetto un corretto e sicuro utilizzo dei medesimi.

2. Le fattispecie di Reato in materia di Delitti informatici e Trattamento illecito dei dati

2.1 I reati presupposto

Di seguito si riporta il testo dell'articolo del codice penale relativo ai reati "presupposto" della responsabilità amministrativa della Società, in relazione ai delitti informatici e trattamento illecito dei dati.

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

1. 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 sino a tre anni.
2. La pena è della reclusione da uno a cinque 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 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 dei dati, delle informazioni o dei programmi in esso contenuti.
3. Qualora i fatti di cui al comma 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 uno a cinque anni e da tre a otto anni.
4. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.)

1. Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna 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 sino ad un anno e con la multa sino ad euro 5.164.
2. La pena è della reclusione da uno a due anni e della multa da euro 5.164 ad euro 10.329 se ricorre taluna delle circostanze di cui al numero 1) e 2) del quarto comma dell'articolo 617 quater.

Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art. 615 quinquies c.p.)

1. Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione totale o parziale, o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino ad euro 10.329.

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

1. Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrente fra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.
2. Salvo che il fatto costituisce 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.
3. I delitti di cui al comma primo e secondo sono punibili a querela della persona offesa.
4. Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:
1. in danno di un sistema informatico o telematico utilizzato dalla Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
2. 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, ovvero con abuso

della qualità di operatore del sistema;
3. da chi esercita anche abusivamente la professione di investigatore privato.

Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.)

1. Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti fra più sistemi, è punito con la reclusione da uno a quattro anni.
2. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617 quater.

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

1. 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 sei mesi a tre anni.
2. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio.

Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 ter c.p.)

1. Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.
2. Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.
3. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

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

1. 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 uno a cinque anni.
2. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies

c.p.)

1. Se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.
2. Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni.
3. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

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

1. 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 euro

Documenti informatici (art. 491 bis c.p.)

1. Se alcune delle falsità previste dal presente capo *(articoli 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490 e 491 codice penale)* riguardano un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private. A tal fine per documento informatico si intende qualunque supporto informatico contenete dati o informazioni aventi efficacia probatoria o specificatamente destinati ad elaborarli.

2.2 Sanzioni

L'articolo 24 bis del D. Lgs. 231/01, introdotto dall'articolo 7 della Legge 18 marzo 2008 n. 48, prevede sanzioni pecuniarie ed interdittive applicabili alla Società in caso di commissione degli illeciti ivi richiamati, nei termini di seguito indicati.

1. In relazione alla commissione dei delitti di cui agli articoli 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater e 635-quinquies del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote.
2. In relazione alla commissione dei delitti di cui agli articoli 615-quater e 615-quinquies del codice penale, si applica all'ente la sanzione pecuniaria sino a trecento quote.
3. In relazione alla commissione dei delitti di cui agli articoli 491-bis e 640-quinquies del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, si applica all'ente la sanzione pecuniaria sino a quattrocento quote.
4. Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste

dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e).

2.3 Esclusione della responsabilità amministrativa della Società

Per una compiuta analisi dei presupposti di cui agli articoli 6 e 7 del Decreto, che consentono di addivenire ad una pronuncia che escluda la responsabilità della Società, si compie un espresso rimando al capitolo 1, paragrafo 4 della Parte Generale del presente Modello.

3. Le "attività sensibili" ai fini del D.Lgs. 231/01

Tali attività sono state individuate con riferimento al complessivo utilizzo dei sistemi informativi di cui la Società è dotata, realizzato mediante l'impiego di sistemi *hardware, software*, di accesso alla rete internet, di utilizzo di sistemi di posta elettronica o di altri sistemi di comunicazione telematica.

La funzione di gestione dei Sistemi Informativi costituisce l'area aziendale che, per le caratteristiche dell'attività e le competenze richieste, è maggiormente esposta al rischio potenziale di incorrere nei reati di cui all'art. *24 bis* del Decreto; tuttavia, non si può realisticamente escludere nessuna area aziendale dal rischio di commettere delitti informatici, nella misura in cui in essa si faccia uso di sistemi *hardware*, *software* e telematici.

In particolare, adeguate procedure e controlli sono previsti per una corretta gestione dell'intero flusso comunicativo e informativo relativo alla Società, sia con riferimento alle informazioni ed ai documenti in fase di ingresso, che a quelli in fase di uscita.

Parimenti è necessario dotarsi di adeguati strumenti che permettano di evitare non solo la perdita di dati e/o informazioni importanti per la Società, ma altresì la loro modifica o alterazione attuata per scopi illeciti attraverso, in primo luogo, la possibilità di risalire con certezza al titolare del documento, rendendo in tal modo individuabile il soggetto a cui il medesimo risulta riconducibile.

Particolare attenzione viene altresì riservata alla necessità di garantire una certa flessibilità del Modello stesso, il quale è opportunamente costituito da una componente *standard*, la quale potrà essere sempre oggetto di modificazione od integrazione alla luce di eventuali evoluzioni della struttura aziendali o di progressi tecnologici in materia.

Infine la Società si impegna a dare adeguata comunicazione delle norme e delle procedure adottate e di organizzare corsi di formazione e aggiornamento su temi specifici o particolarmente complessi.

4. Sistema dei controlli

4.1 Premessa

La Società, nell'adeguare il proprio Modello ai reati in materia di delitti informatici e trattamento illecito dei dati, ha tenuto conto dei seguenti indirizzi:

- delle previsioni del Decreto;
- della vigente disciplina legislativa in materia di protezione dei dati personali di cui al D. Lgs. 196 del 30 giugno 2003;
- del Codice di Comportamento delle imprese di costruzione ai sensi dell'art. 6, comma 3, del Decreto;
- delle Linee Guida Confindustria.

4.2 Principi di comportamento

Tutti i dipendenti ed i collaboratori di Concessioni Autostradali Lombarde S.p.A. destinatari del Modello si devono attenere a principi di ordine generale al fine di prevenire, ed impedire, il verificarsi degli illeciti in materia informatica e di trattamento illecito dei dati.
In particolare essi:

- si astengono dalla falsificazione di qualsiasi documento informatico;
- si astengono dall'effettuare accessi abusivi a sistemi informatici o telematici e dal detenere o diffondere abusivamente codici di accesso a sistemi informatici o telematici;
- non usano né diffondono apparecchiature, dispositivi o programmi informatici che possano in qualsiasi modo danneggiare o interrompere un sistema informatico o telematico;
- si astengono dall'intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche e dall'installare apparecchiature idonee ad intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche;
- non effettuano alcuna attività rivolta al danneggiamento di informazioni, dati e programmi informatici o al danneggiamento di sistemi informatici e telematici;
- si attengono scrupolosamente alle istruzioni operative e alle procedure aziendali diffuse e in uso presso Concessioni Autostradali Lombarde S.p.A.

Ulteriori regole di condotte di portata più specifica devono poi essere osservate da tutti i dipendenti/collaboratori della Società che hanno accesso e che utilizzano il sistema informatico di Concessioni Autostradali Lombarde S.p.A., ai quali viene assegnato un *computer*, portatile o fisso (di proprietà della medesima), al solo scopo di eseguire attività inerente alle mansioni esercitate.

A tutti i destinatari del Modello è vietato

- utilizzare il *computer* a propria disposizione per scopi esclusivamente personali;
- eseguire o tentare di eseguire installazioni di prodotti *software* in proprio possesso senza l'autorizzazione del RSI;
- consentire a soggetti, interni od esterni all'azienda, di accedere al proprio *computer* anche temporaneamente, se non dopo essersi collegato alla rete con il proprio identificativo;

- inserire nel *computer* alcun supporto di memorizzazione esterno tipo:
  - dischi fissi esterni
  - chiavette USB
  - DVD o CD

  qualora i medesimi supporti non siano di provenienza conosciuta e garantita;
- collegare il *computer* aziendale a reti informatiche di cui non si conoscono i dettagli e comunque senza l'autorizzazione del RSI;
- salvare dati al di fuori del proprio profilo utente in modo che siano visibili da altri che si collegano in modo lecito al *computer* con un altro identificativo;
- copiare dati aziendali sui *computer* di casa o su dispositivi rimovibili, qualora non sia strettamente necessario per fini lavorativi;
- inviare per posta elettronica dati sensibili;
- configurare l'accesso remoto a Concessioni Autostradali Lombarde S.p.A. su *computer* diversi da quello in uso;
- consentire a chiunque esterno all'azienda di collegare il proprio *computer* alla rete aziendale senza previa autorizzazione del RSI;
- mantenere attive due connessioni di rete contemporaneamente, tipo la wireless e la connessione via cavo;
- diffondere le proprie credenziali di accesso (login e password) al computer / alla rete aziendale nonché quelle ricevute da terzi (banche dati) in virtù del ruolo svolto per la Società.

Ogni Destinatario del Modello ha invece l'obbligo di:

- bloccare il *computer* mediante la sequenza Crtl+Alt+Canc (blocco del computer) ogni qualvolta si allontana, anche per pochi minuti, dalla propria postazione: tale impostazione si attiverà automaticamente dopo 10 minuti di totale inattività e non sarà disabilitabile dagli utenti;
- evitare di condividere documenti e *file* in genere con il *computer* di casa o di altri;
- utilizzare lo *screen saver* protetto da *password*;
- segnalare tempestivamente al RSI qualsiasi anomalia riconducibile ad un *virus* o ad un attacco informatico;
- utilizzare adeguatamente il *computer* stesso evitando inutili sprechi di traffico dati;
- avvisare immediatamente il RSI qualora sia notato personale presumibilmente non autorizzato che movimenta i cavi di rete, collega apparati di qualunque tipo alla rete informatica e/o telefonica, oppure accede ai locali tecnici;
- avvisare immediatamente il RSI qualora al medesimo venga indebitamente sottratto il proprio *computer* o qualsiasi altro dispositivo utilizzato per connettersi alla rete di Concessioni Autostradali Lombarde S.p.A.;
- avvisare tempestivamente il RSI, anche per il tramite del Responsabile dell'Area Personale, Privacy, Sicurezza, Servizi Generali quando un dipendente/collaboratore di Concessioni Autostradali Lombarde S.p.A. termina il proprio rapporto di collaborazione in modo tale da consentire al RSI di provvedere alla disabilitazione degli accessi;
- conservare le proprie credenziali di accesso (login e password) al computer /rete aziendale e ad eventuali sistemi di terzi conformemente alle regole aziendali.

4.3 Protocolli di controllo

Tutti i Destinatari del Modello, come individuati nel paragrafo 4, capitolo 2 della Parte Generale, adottano regole di condotta conformi:

- ai principi contenuti nel Codice Etico (che qui si intende integralmente richiamato) che costituiscono presupposto e parte integrante dei protocolli di prevenzione di seguito declinati;
- ai protocolli di prevenzione generali previsti dalla Parte Generale;
- ai protocolli di prevenzione specifici di seguito rappresentati.

Prescrizioni per l'accesso alle risorse informatiche

1. Finalità

La presente procedura definisce le strutture informatiche e le relative modalità di accesso alle stesse da parte degli utilizzatori del sistema informativo di Concessioni Autostradali Lombarde S.p.A. Tale procedura deve essere rispettata da tutti gli utenti, indipendentemente dal luogo in cui si trovano e dalle risorse che utilizzano per connettersi al sistema informativo.

2. Definizioni

Risorse informatiche**:** i mezzi informatici della Società accessibili attraverso la rete aziendale.
Risorse di rete**:** l'insieme dei servizi forniti da *server* locali o remoti, riguardanti mezzi di informazioni diversi: *file server*, posta elettronica, *internet*, etc.
Amministratori di sistema (RSI)**:** i tecnici del settore IT che hanno l'incarico di installare e gestire i sistemi informatici della rete al fine di assicurarne il miglior funzionamento possibile.
Identificativo Utente o account**:** nome univoco che permette di identificare l'utente quando accede alle risorse informatiche, tipicamente composto dal nome e dal cognome dell'utente separati da un punto (.).
Parola chiave o *password***:** parola o sigla di riconoscimento fornita dall'utente al sistema per poter accedere alle risorse informatiche e di rete.

3. Responsabilità

La presente procedura deve essere rispettata da tutti gli utenti del sistema informativo di Concessioni Autostradali Lombarde S.p.A.
I servizi messi a disposizione dal RSI devono essere utilizzati unicamente per gli scopi e le finalità aziendali.
Il RSI in particolare deve:

- attivare i livelli di sicurezza per i diversi servizi;
- assicurare il controllo dei sistemi;
- informare gli utenti circa i possibili rischi derivanti dall'uso scorretto delle risorse informatiche.

4. Accesso alla rete

L'accesso alla rete di Concessioni Autostradali Lombarde S.p.A. è riservato agli utenti autorizzati (di norma dipendenti e collaboratori) e presuppone una autorizzazione che definisca i limiti e le condizioni di accesso.

4.1 Modalità di utilizzo

Il RSI attribuisce le credenziali di accesso, ovvero una *login* ed una *password* di accesso a ciascun utente che deve essere modificata dall'utente stesso immediatamente dopo il primo accesso. L'utilizzo delle risorse informatiche e di rete è autorizzato esclusivamente per scopi attinenti l'attività di lavoro degli utenti.
Ogni utente è responsabile del corretto uso delle risorse informatiche e di rete alle quali ha accesso. L'uso delle risorse deve rispondere alle disposizioni dettate da RSI al fine di evitarne la saturazione e un uso improprio.

5. Accesso al servizio di posta elettronica
L'accesso al servizio di posta elettronica aziendale *è* riservato ai dipendenti/collaboratori ed alle persone autorizzate. Il RSI provvede a creare la Mailbox Utente.

5.1 Modalità di utilizzo
Il sistema di posta elettronica di proprietà della Società deve essere usato esclusivamente per motivi di lavoro; ogni dipendente/collaboratore è responsabile del corretto uso della stessa.

6. Accesso al servizio internet
L'accesso ad *internet* attraverso i sistemi aziendali è riservato ai dipendenti/collaboratori e alle persone autorizzate che per lo svolgimento del proprio lavoro necessitano di tale collegamento.

6.1 Modalità di utilizzo
La navigazione in *internet* può essere utilizzata solo per scopi inerenti l'adempimento del proprio lavoro.
L'utente è direttamente responsabile, civilmente e penalmente, per l'uso improprio di Internet, per la violazione di accessi protetti, per il mancato rispetto delle norme sul *copyright* e sulle licenze d'uso. Non è altresì consentito:

- svolgere operazioni che influenzino o compromettano la regolare operatività della rete o ne restringano la funzione e le prestazioni;
- scaricare *software* da i*nternet* senza autorizzazione da parte del RSI;
- utilizzare *software* autonomamente installati allo scopo di connettersi a *Chat*, messaggerie esterne e *mailbox* personali.

7.Accesso remoto alla rete aziendale

L'accesso alla rete in modalità remota è riservato ai dipendenti e alle persone autorizzate che abbiano necessità di collegarsi ai server aziendali dall'esterno, ove non siano disponibili accessi diretti alla rete stessa, ovvero ove non si disponga della rete geografica.

7.1 Modalità di utilizzo
L'accesso alla rete è attualmente consentito solo mediante connessioni VPN via Internet con autenticazione mediante certificato digitale.
Gli utenti che si trovano in sedi collegate nella rete geografica di Concessioni Autostradali Lombarde S.p.A. non dovranno usare la connettività via VPN in quanto esistono già

connessioni VPN LAN - to - LAN. Quando la connessione VPN avviene mediante scheda Vodafone, il costo è abbastanza sensibile, pertanto tutti gli utenti sono invitati ad utilizzare tale connessione solo quando strettamente necessario e per il solo periodo di tempo per cui è indispensabile.

Si raccomanda anche di evitare il più possibile di scaricare file di dimensioni superiori ad 1 MB, di navigare su *internet* e di accedere ai *file* in rete se non più che indispensabile.

Per motivi di sicurezza *è* necessario che:

- il PC sia scollegato da eventuali altre interfacce di rete e/o altri sistemi informativi di altre aziende;
- durante il collegamento il PC sia sempre presidiato ed eventualmente bloccato se lasciato anche per poco incustodito.

In ogni caso l'utente è responsabile degli eventuali danni che un non corretto uso dell'accesso remoto possono derivare alla società.

Non è inoltre consentito attivare accessi remoti dall'interno di una struttura aziendale se il PC è connesso alla rete locale, ovvero collegarsi ad altri sistemi mentre si è collegati al sistema informativo di Concessioni Autostradali Lombarde S.p.A., così come collegare alla rete locale ogni forma di apparato che possa consentire accessi indesiderati tipo *access point wireless*, *bridge bluetooth* e quant'altro.

8. Sicurezza ed integrità dei dati

Ogni utente deve contribuire alla sicurezza complessiva del sistema.
In particolare deve:

- applicare le norme di sicurezza definite dalla Società;
- assicurare la protezione del proprio *account*, della *password* e dei propri *file*;
- segnalare agli amministratori del sistema ogni tentativo di violazione del suo *account* e le eventuali anomalie constatate;
- disconnettersi dalla rete e spegnere il computer prima di lasciare l'ufficio.

8.1 Password

Le *password* di accesso devono essere adeguatamente protette per garantire la riservatezza dei dati.
Gli utenti devono scegliere la *password* senza interventi dell'amministratore né di altre persone, ed in particolare:

- le *password* degli utenti devono avere una lunghezza minima di 8 caratteri ed una scadenza non superiore a 60 giorni;
- le *password* non devono essere facilmente riconoscibili (non utilizzare quindi date di nascita o nome/cognome, etc.) devono contenere sia caratteri numerici che alfabetici;
- le *password* non devono essere condivise con altri, ma devono essere conosciute solo dall'utente;
- le *password* di accesso alla rete e della casella di posta elettronica devono essere cambiate frequentemente e, in ogni caso, quando il sistema lo richieda.

Nel caso in cui la *password* iniziale sia stata scelta dall'amministratore, essa dovrà essere modificata al momento del primo accesso al sistema.

8.2 Salvaguardia dei dati personali
Gli utenti sono responsabili dei back-up dei dati e dei folders residenti sul personal computer assegnato.
Per qualsiasi esigenza è possibile rivolgersi al RSI.

8.3 Protezione Antivirus
Tutti i PC aziendali sono protetti da un programma Antivirus che viene attivato automaticamente al momento dell'accensione del PC.
Compito dell'utente è quello di verificare l'eventuale presenza di virus, eseguendo periodicamente il programma antivirus sul proprio PC e talvolta verificarne l'avvenuto aggiornamento.
Il RSI ha il compito di garantire l'assenza di virus sui server di rete e di controllare le aree di sistema ed applicative.

9 Controlli
Gli amministratori di sistema hanno tutti i poteri per sorvegliare il corretto uso del sistema informatico, tutto ciò senza consultare i contenuti dei dati stessi, ma solamente verificando la loro esistenza.
Gli amministratori di sistema devono consultare tutti i *log* di sistema e registrarne degli estratti al fine di poter garantire le piene funzionalità del sistema stesso.
Solo mediante una lettura precisa e frequente dei *log* si può garantire la sicurezza e l'affidabilità del sistema.
In caso di attacchi di pirateria informatica o per quei casi in cui il buon funzionamento e la sicurezza del sistema lo richiedano, gli amministratori possono porre in atto tutti gli adempimenti necessari all'individuazione delle cause e riferire direttamente alla Direzione Generale.

Prescrizioni per la gestione delle risorse informatiche condivise

1. Finalità
La presente procedura descrive in modo semplice e dettagliato le strutture dei dati disponibili per tutti gli utenti di Concessioni Autostradali Lombarde S.p.A., affinché siano utilizzate nel migliore dei modi e garantendo la massima sicurezza.

2. Responsabilità
La procedura deve essere applicata da tutti gli utenti del sistema informativo di Concessioni Autostradali Lombarde S.p.A..
I servizi messi a disposizione dal RSI devono essere utilizzati unicamente per gli scopi e le finalità aziendali.
Il RSI in particolare deve:
- attivare i livelli di sicurezza per i diversi servizi;
- assicurare il controllo dei sistemi;
- informare gli utenti circa i possibili rischi derivanti dall'uso scorretto delle risorse informatiche.

3. Elenco e descrizione delle risorse

Le principali risorse condivise tra gli utenti di Concessioni Autostradali Lombarde S.p.A. sono:
Disco K: è il disco che contiene i documenti relativi alle commesse, ai lavori in corso e tutto ciò che viene normalmente utilizzato dagli utenti dell'area tecnica. Il contenuto di tale disco viene salvato ogni notte su nastro magnetico. E' indispensabile che, per una ottimale gestione, il disco non contenga *file* copiati temporaneamente, duplicati e tutto quanto contribuisce ad aumentarne senza scopo le sue dimensioni.
Disco T: è il disco preposto per lo scambio dei file tra gli utenti del sistema informativo di Concessioni Autostradali Lombarde S.p.A. Tale disco non deve essere utilizzato per memorizzare in modo permanente i dati, ma solo per consentire uno scambio agevole dei documenti evitando l'utilizzo della posta elettronica. L'utente, una volta ricevuti i *file*, provvede a spostarli dal disco T: alla destinazione che ritiene più idonea, in genere una cartella del proprio disco fisso.
E' importante ricordare che il contenuto del disco T non viene mai salvato dai processi di *back-up*.
Disco U: ciascun utente ha un disco U: automaticamente assegnato alla propria utenza. Tale disco serve per memorizzare file di lavoro che non vengono condivisi con altri utenti, ma che devono essere preservati anche in caso di rottura del proprio computer. Non si devono salvare nel disco U: file personali, musica, fotografie e tutto quanto contribuisce ad appesantire i processi di back-up.
PST: è una risorsa condivisa non visibile direttamente sotto forma di disco, ma che contiene tutte le cartelle utente con archivi di posta elettronica.
Al fine di evitare perdite di informazioni è importante che tutti gli utenti dotati di *computer* non portatili memorizzino in tale *location* i propri archivi di posta elettronica, che saranno regolarmente salvati dai *back-up*. Gli utenti di *computer* portatili possono scegliere se mantenere anch'essi i *file* di archivio in tale *location* non potendone disporre quando *offline*, o se mantenerli sul proprio computer facendosi carico della loro gestione e del loro salvataggio. Il RSI è a disposizione per facilitare tale scelta e/o per fornire aiuto per l'implementazione.

4 Denominazione dei documenti
I documenti contenuti nelle risorse di rete devono rispettare alcune regole fondamentali per evitare che possano non essere più reperibili, salvabili dai processi *di back-up*, subire danni etc.

- I documenti possono essere di qualunque tipo.
- I file non devono avere nomi più lunghi di 50 caratteri circa.
- I nomi devono contenere solo i caratteri alfanumerici dell'alfabeto internazionale e non più di un carattere "." che separa il nome del file dall'estensione. L'utilizzo dei caratteri speciali (virgole, parentesi, simboli etc.) non garantisce il normale utilizzo dei file.

I percorsi nei quali sono contenuti i documenti non devono essere più lunghi di 200 caratteri (compresi quelli di separazione): il nome del percorso e quello dei *file* non deve pertanto superare la lunghezza totale di 250 caratteri.

Prescrizioni per la gestione della posta elettronica

1. Finalità

La presente istruzione operativa ha lo scopo di definire le modalità di funzionamento del sistema di posta elettronica di Concessioni Autostradali Lombarde S.p.A. , evidenziandone le caratteristiche principali, le funzionalità, le corrette modalità di utilizzo e le limitazioni imposte al fine di garantire la sicurezza ed il funzionamento dei servizi ad essa collegati.

2. Caratteristiche

Il sistema di posta elettronica di Concessioni Autostradali Lombarde S.p.A. è stato pensato e realizzato per consentire ai suoi utenti lo scambio di messaggi di posta con o senza allegati e la condivisione di informazioni utili per il lavoro, sia localmente sia da remoto.
Ogni utente del sistema aziendale ha almeno un proprio indirizzo di posta nel formato:
nome.cognome@calspa.it
A tale indirizzo corrisponde una casella postale analoga, dal punto di vista concettuale, alla cassetta della posta convenzionale, all'interno della quale ciascun utente può memorizzare informazioni relative a:

- Messaggi di posta elettronica
- Appuntamenti
- Rubrica con nomi, indirizzi e numeri telefonici
- Note
- Task da gestire

Tutti i dati contenuti all'interno della casella sono di esclusiva proprietà dell'utente che la gestisce; tali dati non possono essere visualizzati da altre persone senza l'autorizzazione del legittimo proprietario.
Per una più completa gestione delle informazioni gli utenti possono condividere tutta o parte della propria casella con i colleghi, attribuendo ad ognuno gli opportuni privilegi su ogni livello della casella stessa.
Un'altra semplice funzionalità utilizzata è quella di condividere delle cartelle pubbliche che possono contenere dati relativi ad appuntamenti, contatti o messaggi di posta divisi per argomento, commessa o quanto altro utile per migliorare e snellire le procedure operative del lavoro quotidiano.

3. Sicurezza

Il software sul quale si basa il sistema di posta elettronica è Microsoft Exchange Server, il migliore oggi a disposizione, che offre vari livelli di sicurezza per soddisfare le esigenze di tutte le fasce di utenza.
In Concessioni Autostradali Lombarde S.p.A. si è deciso di basare la sicurezza negli accessi sulle credenziali di rete, ovvero nome utente e relativa password associata, gestite con le modalità conformi alle norme in vigore.

3.1 Protezione contro la perdita di dati

Utilizzando Outlook è possibile recuperare i dati erroneamente cancellati attingendo direttamente dal cestino.
Il sistema Exchange consente inoltre di recuperare qualsiasi elemento dalle caselle - cestino compreso - entro 7 giorni dalla data della cancellazione direttamente dall'Outlook dell'utente o con l'aiuto dei sistemi informativi.
Come ultimo sistema di sicurezza contro la perdita dei dati viene utilizzato il back-up, eseguito tutte le notti dal lunedì al venerdì e che consente di recuperare elementi cancellati in qualunque momento e rimasti nella casella per almeno una giornata intera.

4. Garanzie di funzionamento

E' importante sapere che la ricezione di un messaggio di posta elettronica di qualunque tipo via Internet NON è garantito o garantibile da nessuno e da nessun sistema.
Solitamente almeno il 99,9% dei messaggi arriva regolarmente a destinazione ed anche in tempi brevissimi, ma le regole di internet stabiliscono quanto sopra citato e non sono modificabili dai provider o altre entità.
L'invio di un messaggio ad utenti del sistema interno è invece garantito dal fatto stesso che il mittente compone il messaggio, quindi non è utile richiedere al sistema le ricevute che confermino l'invio, in quanto l'avere la possibilità di premere il tasto "Invia" rappresenta già la garanzia.
Può invece essere utile richiedere la ricevuta di lettura, come prova che il messaggio sia stato letto, sia internamente che esternamente.
Tale ricevuta è garantita solo per corrispondenti interni, mentre non tutti i sistemi Internet sono configurati per inviare le ricevute lettura ad utenti esterni al proprio sistema.
Il sistema di Concessioni Autostradali Lombarde S.p.A. invia, senza limitazioni, sia le ricevute di lettura che quelle di errore di spedizione (tecnicamente i Non Delivery Reports) anche agli utenti esterni.

5. Limitazioni imposte per motivi di sicurezza

Negli ultimi anni i sistemi di posta elettronica sono stati spesso utilizzati come veicolo per trasmettere virus, messaggi non graditi, avvisi commerciali ecc.: si è reso pertanto necessario installare dei sistemi che controllino automaticamente i messaggi e li scartino sulla base di determinati requisiti impostati dagli amministratori del sistema.
Non si tratta di sistemi che leggono il contenuto dei messaggi in arrivo e lo inviano ad altri, bensì di strumenti che ne leggono il contenuto alla ricerca di informazioni predefinite che servono per catalogarlo come sgradito (SPAM o Junk) o lecito (HAM).
Questi sistemi, una volta configurati ed attivati, funzionano molto bene ma non sono in grado di definire la sicurezza e legittimità del messaggio: può pertanto succedere che qualche messaggio venga erroneamente catalogato come SPAM.
A questo scopo il sistema avvisa il destinatario che un messaggio a lui destinato è stato spostato in una sorta di quarantena in quanto ritenuto indesiderato, e gli consente di contattare gli amministratori per l'eventualmente ripristino.
Si ricorda una regola generale molto importante ai fini della sicurezza informatica: un messaggio inviato da una persona ben conosciuta può contenere SPAM; la discriminante da prendere in considerazione, infatti, non è tanto l'affidabilità generale del mittente (che non viene certamente messa in discussione), bensì quella del sistema informativo dal quale scrive.
Per citare un esempio, una mail spedita da un indirizzo di tin.it, virgilio.it, libero.it, tiscali.it ecc., ha più probabilità di essere pericoloso di uno inviato da un sistema di posta corporate come quello di Concessioni Autostradali Lombarde S.p.A.

6. Gestione degli allegati e degli archivi di posta elettronica

L'invio e la ricezione degli allegati è consentito tranne che per quelle tipologie che possono essere particolarmente pericolose, come i programmi eseguibili (.EXE .COM .BAT, .CMD) etc. i quali, se ricevuti, possono causare danni al sistema.
La dimensione massima degli allegati, sia in spedizione che in ricezione, è stata fissata per tutti in 10 Mbyte.

Tale valore risulta già essere molto superiore alla prassi in quanto la posta non è per definizione il miglior sistema di trasporto per documenti di dimensioni superiori a qualche Mb.
Qualora fosse necessario trasmettere documenti di dimensioni superiori è possibile nell'ordine agire come segue:

1. dividere i documenti da spedire in più messaggi;
2. comprimere gli allegati utilizzando programmi tipo Winzip o Winrar o il compressore incluso in Windows;
3. utilizzare il sistema delle aree condivise sul sito web, rivolgendosi anticipatamente agli amministratori di sistema se si tratta della prima volta;
4. rivolgersi agli amministratori.

Per quanto attiene la gestione degli archivi di posta elettronica, dal momento che è stato fissato un limite di 500 Mb di spazio per ogni casella di posta, è necessario provvedere all'archiviazione dei messaggi prima del raggiungimento di suddetta soglia.
A questo scopo è possibile creare un personal folder file che può contenere esattamente la stessa struttura della casella di posta. Tale file, se risiede sul pc dell'utente, non è salvato dai back-up del sistema e potrebbe venire distrutto in caso di crash del disco fisso: si raccomanda, pertanto, di masterizzare una copia del file o di rivolgersi a RSI per assistenza.