PBM Atletica Leggera – Bovisio Masciago
Associazione Sportiva Dilettantistica

PROGETTO DI PROTEZIONE DEI DATI PERSONALI ai sensi del regolamento UE 2016/679

parte speciale
allegato 6
Linee guida per il corretto utilizzo degli strumenti elettronici

[20190127]

SOMMARIO

1. PREMESSA

La normativa italiana classifica l'uso dei computer e, in generale, degli strumenti informatici tra le attività pericolose ai sensi dell'articolo 2050 del Codice Civile e questo comporta delle responsabilità specifiche sia per le persone che li utilizzano sia per le organizzazioni che ne sono proprietarie.
Anche dal punto di vista penale, l'attività svolta con i computer ha assunto una rilevanza particolare: all'art. 615 quinquies del Codice Penale, ad esempio, sono elencate delle fattispecie, tra cui la diffusione di virus e il danneggiamento di sistemi e di reti telematiche, alle quali sono associate responsabilità e pene specifiche.
Di seguito si riporta il testo dell'art. 615quinquies c.p.

Articolo 615 Quinquies c.p.
Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico - *Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, 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, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.*

A ciò deve aggiungersi che a far data dal 2001, con l'entrata in vigore del D. Lgs. 231/2001, è stata estesa la responsabilità agli enti (ovvero la responsabilità per le società e le persone giuridiche, enti ed associazioni in generale) prevedendo l'applicabilità di sanzioni pecuniarie ed interdittive in caso di compimento di determinati reati nell'interesse e a vantaggio degli enti stessi. Ai fini del presente documento giova rammentare in particolare che a partire dal 2008, con l'introduzione dell'art. 24-bis del D. Lgs. 231/2001, tale responsabilità "penale" delle società è stata estesa anche ai reati informatici relativi a accesso abusivo ad un sistema informatico o telematico, intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche, installazione di apparecchiature per intercettare, impedimento o interruzione di comunicazioni informatiche o telematiche, danneggiamento di informazioni, dati o programmi informatici, danneggiamento di sistemi informatici o telematici, detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici, diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico, frode informatica del soggetto che presta servizi di certificazione di firma elettronica, documenti informatici.
Tale dettato normativo impatta evidentemente sull'utilizzo degli strumenti informatici e sul trattamento dei dati con strumenti informatici in azienda che devono pertanto – giocoforza – essere disciplinati in dettaglio dall'azienda stessa.
Si riporta di seguito una descrizione dei reati richiamati dall'art. 24-bis del d.lgs. 231/2001.

Delitti informatici e trattamento illecito di dati (Art. 24-bis, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 48/2008; modificato dal D.Lgs. n. 7 e 8/2016]

Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491-bis c.p.) – "*Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti gli atti pubblici"*
Questo reato si realizza nel caso di compimento di una condotta illecita di falso relativamente a documenti informatici pubblici o privati aventi efficacia probatoria. In particolare, le falsità concernenti documenti e atti informatici rilevano ai fini del d. lgs. 231/2001, se riferite alle disposizioni indicate dal capo stesso e riferite agli atti pubblici e alle scritture private, che per semplicità, si riportano di seguito.

- ***art. 476 c.p. - falsità materiale commessa dal pubblico ufficiale in atti pubblici:*** *vi incorre il pubblico ufficiale, che, nell'esercizio delle sue funzioni, forma, in tutto o in parte, un atto falso o altera un atto vero, è punito con la reclusione da uno a sei anni. Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a dieci anni.*
- ***art. 477 c.p. - falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative:*** *vi incorre il pubblico ufficiale, che, nell'esercizio delle sue funzioni, contraffà o altera certificati o autorizzazioni amministrative, ovvero, mediante contraffazione o alterazione, fa apparire adempiute le condizioni richieste per la loro validità, è punito con la reclusione da sei mesi a tre anni.*
- ***art. 478 c.p. - falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti:*** *vi incorre il pubblico ufficiale, che, nell'esercizio delle sue funzioni, supponendo esistente un atto pubblico o privato, ne simula una copia e la rilascia in forma legale, ovvero rilascia una copia di un atto pubblico o privato diversa dall'originale, è punito con la reclusione da uno a quattro anni. Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a otto anni. Se la falsità è commessa dal pubblico ufficiale in un attestato sul contenuto di atti, pubblici o privati, la pena è della reclusione da uno a tre anni.*
- ***art. 479 c.p. - falsità ideologica commessa dal pubblico ufficiale in atti pubblici:*** *vi incorre il pubblico ufficiale, che, ricevendo o formando un atto nell'esercizio delle sue funzioni, attesta falsamente che un fatto è stato da lui compiuto o è avvenuto alla sua presenza, o attesta come da lui ricevute dichiarazioni a lui non rese, ovvero omette o altera dichiarazioni da lui ricevute, o comunque attesta falsamente fatti dei quali l'atto è destinato a provare la verità, soggiace alle pene stabilite nell'articolo 476*
- ***art. 480 c.p. - falsità ideologica commessa dal pubblico ufficiale in certificati o in autorizzazioni amministrative:*** *vi incorre il pubblico ufficiale, che, nell'esercizio delle sue funzioni, attesta falsamente, in certificati o autorizzazioni amministrative, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione da tre mesi a due anni.*
- ***art. 481 c.p. - falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità:*** *vi incorre chiunque, nell'esercizio di una professione sanitaria o forense, o di un altro servizio di pubblica necessità, attesta falsamente, in un certificato, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a un anno o con la multa da Euro 51,00 a Euro 516,00. Tali pene si applicano congiuntamente se il fatto è commesso a scopo di lucro.*
- ***art. 482 c.p. - falsità materiale commessa dal privato:*** *se alcuno dei fatti preveduti dagli articoli 476, 477 e 478 è commesso da un privato, ovvero da un pubblico ufficiale fuori dell'esercizio delle sue funzioni, si applicano rispettivamente le pene stabilite nei detti articoli, ridotte di un terzo.*
- ***art. 483 c.p. - falsità ideologica commessa dal privato in atto pubblico:*** *vi incorre chiunque attesta falsamente al pubblico ufficiale, in un atto pubblico, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a due anni. Se si tratta di false attestazioni in atti dello stato civile, la reclusione non può essere inferiore a tre mesi.*
- ***art. 484 c.p. - falsità in registri e notificazioni:*** *vi incorre chiunque, essendo per legge obbligato a fare registrazioni soggette all'ispezione dell'Autorità di pubblica sicurezza, o a fare notificazioni all'Autorità stessa circa le proprie operazioni industriali, commerciali o professionali, scrive o lascia scrivere false indicazioni è punito con la reclusione fino a sei mesi o con la multa fino a Euro 309,00.*
- ***art. 485 c.p. - falsità in scrittura privata:*** *vi incorre chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, forma, in tutto o in parte, una scrittura privata falsa, o altera una scrittura privata vera, è punito, qualora ne faccia uso o lasci che altri ne faccia uso, con*

la reclusione da sei mesi a tre anni. Si considerano alterazioni anche le aggiunte falsamente apposte a una scrittura vera, dopo che questa fu definitivamente formata.

- ***art. 486 c.p. - falsità in foglio firmato in bianco. atto privato:*** *vi incorre chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, abusando di un foglio firmato in bianco, del quale abbia il possesso per un titolo che importi l'obbligo o la facoltà di riempirlo, vi scrive o fa scrivere un atto privato produttivo di effetti giuridici, diverso da quello a cui era obbligato o autorizzato, è punito, se del foglio faccia uso o lasci che altri ne faccia uso, con la reclusione da sei mesi a tre anni. Si considera firmato in bianco il foglio in cui il sottoscrittore abbia lasciato bianco un qualsiasi spazio destinato a essere riempito.*
- ***art. 487 c.p. - falsità in foglio firmato in bianco. atto pubblico:*** *vi incorre il pubblico ufficiale, che, abusando di un foglio firmato in bianco, del quale abbia il possesso per ragione del suo ufficio e per un titolo che importa l'obbligo o la facoltà di riempirlo, vi scrive o vi fa scrivere un atto pubblico diverso da quello a cui era obbligato o autorizzato, soggiace alle pene rispettivamente stabilite negli articoli 479 e 480.*
- ***art. 488 c.p. - altre falsità in foglio firmato in bianco. applicabilità delle disposizioni sulle falsità materiali:*** *ai casi di falsità su un foglio firmato in bianco diversi da quelli preveduti dai due articoli precedenti, si applicano le disposizioni sulle falsità materiali in atti pubblici o in scritture private.*
- ***art. 489 c.p. uso di atto falso:*** *vi incorre chiunque senza essere concorso nella falsità, fa uso di un atto falso soggiace alle pene stabilite negli articoli precedenti, ridotte di un terzo. Qualora si tratti di scritture private, chi commette il fatto è punibile soltanto se ha agito al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno.*
- ***art. 490 c.p. soppressione, distruzione e occultamento di atti veri:*** *vi incorre chiunque, in tutto o in parte, distrugge, sopprime od occulta un atto pubblico o una scrittura privata veri soggiace rispettivamente alle pene stabilite negli articoli 476, 477, 482 e 485, secondo le distinzioni in essi contenute. Si applica la disposizione del capoverso dell'articolo precedente.*
- ***art. 492 c.p. copie autentiche che tengono luogo degli originali mancanti:*** *agli effetti delle disposizioni precedenti, nella denominazione di "atti pubblici" e di "scritture private" sono compresi gli atti originali e le copie autentiche di essi, quando a norma di legge tengano luogo degli originali mancanti.*
- ***art. 493 c.p. - falsità commesse da pubblici impiegati incaricati di un servizio pubblico:*** *le disposizioni degli articoli precedenti sulle falsità commesse da pubblici ufficiali si applicano altresì agli impiegati dello Stato, o di un altro ente pubblico, incaricati di un pubblico servizio relativamente agli atti che essi redigono nell'esercizio delle loro attribuzioni.*

*

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 fino 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 palesmente 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 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 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".

Questo reato si realizza tramite la condotta di un soggetto che si introduce abusivamente 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.
Si precisa che:

- si tratta di reato comune, la cui condotta può essere realizzata da chiunque;
- per la fattispecie sopraccitata, la pena è generalmente della reclusione fino a tre anni e il delitto si punisce a querela della persona offesa;
- la pena è, invece, della reclusione da uno a cinque anni e si procede d'ufficio:
  1) se il fatto e' 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 e' 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;

La pena è della reclusione da uno a cinque anni e da tre a otto anni, nonché si procede d'ufficio, se, rispettivamente, l'introduzione abusiva o il mantenimento contro la volontà dell'avente diritto, 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.

*

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 a euro 5.164. [2] La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1 e 2 del quarto comma dell'articolo 617 quater".*

La fattispecie si concretizza allorquando un soggetto, 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.

Si precisa che:

- si tratta di reato comune, la cui condotta può essere realizzata da chiunque;
- la pena è della reclusione sino ad un anno e della multa sino a 5.164 euro, aumentata se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617 quater.

*

Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.) – "*[1] Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, 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, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329".*

Il reato consiste nella condotta messa in atto da soggetto che, allo scopo di danneggiare illecitamente un sistema informatico o telematico, 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, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici.

Si precisa che:

- si tratta di reato comune, la cui condotta può essere realizzata da chiunque;
- la pena è della reclusione sino a due anni e della multa sino a euro 10.329 euro.

*

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 intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni. [2] 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.[3] I delitti di cui ai commi 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 dallo 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"*

Tale reato consiste nell'intercettazione, nell'impedimento o nell'interruzione fraudolenta di comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi.
Si precisa che:

- si tratta di reato comune, la cui condotta può essere realizzata da chiunque;
- la pena è della reclusione da sei mesi a quattro 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 sopraccitate comunicazioni;
- i delitti sono punibili a querela della persona offesa.

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 dallo 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 tra 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"*

Questo reato condanna la condotta di quei soggetti che, fuori dai casi consentiti dalla legge, installano apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi.
Si precisa che:

- si tratta di reato comune, la cui condotta può essere realizzata da chiunque;
- la pena è della reclusione da uno a quattro anni; mentre 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 il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni".*
Il reato condanna la condotta dei soggetti che distruggono, deteriorano, cancellano, alterano o sopprimono informazioni, dati o programmi informatici altrui.
Si precisa che:

- si tratta di reato comune, la cui condotta può essere realizzata da chiunque;
- salvo che il fatto costituisca più grave reato, la pena è della reclusione da sei mesi a tre anni e si procede a querela della persona offesa; se ricorre una o più delle circostanze 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 e' 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 il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di

operatore del sistema, la pena è aumentata".
Tale condotta criminosa consiste nella commissione di 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.
Si precisa che:

- si tratta di reato comune, la cui condotta può essere realizzata da chiunque;
- la pena è della reclusione da uno a quattro anni; 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;
- 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 il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata"*
Tale delitto punisce la condotta del soggetto che, mediante le condotte di cui all'art. 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.
Si precisa che:

- si tratta di reato comune, la cui condotta può essere realizzata da chiunque;
- salvo che il fatto costituisca più grave reato, la pena è della reclusione da uno a cinque anni;
- 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 il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata"*
Strutturalmente questa ipotesi criminosa è simile a quella trattata al punto precedente, ad eccezione del fatto che le sopraccitate condotte sono dirette a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.
Si precisa che:

- si tratta di reato comune, la cui condotta può essere realizzata da chiunque;
- la pena è della reclusione da uno a quattro anni;
- 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;
- 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 certificatore 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*"
Il reato si concretizza qualora 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.
Si precisa che la pena è della reclusione fino a tre anni e della multa da 51 a 1.032 euro.

L'utilizzo di strumenti elettronici e cartacei per il trattamento dei dati forniti a P.B.M. Polisportiva Bovisio Masciago ASD dai suoi interlocutori, siano essi clienti, fornitori, collaboratori, dipendenti o altro, è inoltre vincolato al rispetto delle normative in essere (legali, fiscali, amministrative, eccetera), compresa quella sulla tutela dei dati personali. In aggiunta è fondamentale che gli strumenti e le risorse di P.B.M. Polisportiva Bovisio Masciago ASD siano finalizzati al mantenimento, nel tempo, di un adeguato livello di sicurezza per la conservazione e la protezione dei dati.
Per tali ragioni nel presente documento sono indicate le regole di comportamento interne adottate da P.B.M. Polisportiva Bovisio Masciago ASD volte a salvaguardare sia gli utenti sia P.B.M. Polisportiva Bovisio Masciago ASD dalla possibilità che possano verificarsi nell'ambito dell'attività aziendale fatti illeciti e/o pericolosi nelle operazioni di trattamento di dati per mezzo di strumenti elettronici.
Il presente documento descrive le politiche generali di sicurezza che P.B.M. Polisportiva Bovisio Masciago ASD ha deciso di adottare in tema di utilizzo di posta elettronica e internet sulla base delle Linee Guida del garante e della prassi instauratesi nella vigenza del d.lgs 196/2003.
Il presente documento viene redatto dal Consiglio di Amministrazione ed è soggetto ad aggiornamento periodico coerentemente con l'aggiornamento del documento programmatico di sicurezza nonché all'esposizione tramite consegna cartacea ai dipendenti.
Ogni dipendente e collaboratore di P.B.M. Polisportiva Bovisio Masciago ASD è tenuto a prenderne atto, osservarne i contenuti ed a conformarvi il proprio comportamento. **Qualsiasi comportamento che disattenda quanto ivi contenuto sarà sanzionabile disciplinarmente**.

2. REGOLE GENERALI

Le regole descritte nel presente documento hanno valenza generale e vanno quindi applicate indipendentemente dallo strumento e/o dai dati presi in considerazione.

2.1. Trattamento dei dati

Per quanto riguarda il trattamento dei dati occorre che l'incaricato/utente per quanto possibile:

- eviti di trattare dati sensibili (particolari categorie di dati ex art. 9 GDPR) o dati giudiziari fatto salvo che l'utente stesso svolga mansioni che ne richiedano l'utilizzo oppure nei casi di comprovata necessità.
- informi tempestivamente un amministratore qualora l'utente stesso riceva o entri in possesso o diffonda erroneamente informazioni (tramite, ad esempio, posta elettronica o supporto magnetico) di competenza non sua e/o del reparto di appartenenza;
- possa dimostrare in ogni momento di aver agito con la massima diligenza e con tutti i mezzi a sua disposizione al fine di preservare la sicurezza del patrimonio dati aziendale, attenendosi scrupolosamente alle disposizioni ricevute dagli amministratori.

3. DEFINIZIONI

3.1. Incaricato al trattamento/Utente

Per utente si intende una persona fisica addetta, a qualsiasi titolo, al trattamento di dati aziendali e, nella pratica, si intendono tutti i dipendenti ed i collaboratori di P.B.M. Polisportiva Bovisio Masciago ASD

3.2. Trattamento

Si intende qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

3.3. Responsabile del trattamento

Si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

3.4. Titolare del trattamento

Si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di

dati personali, ivi compreso il profilo della sicurezza, nello specifico P.B.M. Polisportiva Bovisio Masciago ASD.

3.5. PDL

Si definisce postazione di lavoro (in seguito Pdl) una locazione stabile o mobile dalla quale l'incaricato è in grado di interagire con il sistema informativo aziendale in maniera diretta o indiretta.
Per accesso in via indiretta al sistema informativo aziendale si intende la possibilità per l'incaricato di operare su dati memorizzati su apparecchiature fornite insieme alla Pdl aziendale, anche in mancanza di un collegamento diretto. La Pdl è normalmente composta da un personal computer (PC) da tavolo (desktop) o portatile (laptop) e può essere costituita da altri strumenti idonei al trattamento dei dati come per esempio:

- stampante;
- tablet;
- smartphone.

3.6. Dati

Si intendono per dati, tutte le tipologie utilizzate all'interno dell'azienda sia attraverso strumenti elettronici che cartacei. Per maggiori dettagli ci si riferisca al materiale in materia di trattamento dei dati, fornito in sede di assunzione/formazione.
Fanno parte dei dati di pertinenza dell'azienda anche quelli relativi alla struttura organizzativa dell'azienda stessa ed alla configurazione Hardware (HW) e Software (SW) degli strumenti che compongono il sistema informativo dell'azienda (computer, stampanti, programmi, user-id, password, etc.) e degli impianti di ricerca e sviluppo e produzione.

3.7. Incaricato

Per incaricato si intende qualsiasi dipendente e/o collaboratore e/o consulente esterno che acceda ad una Pdl per via delle mansioni attribuite e/o degli incarichi affidati. Questo ha valore quindi anche per i collaboratori e/o consulenti esterni che accedono a PdL messe a disposizione dall'azienda.

4. DISPOSIZIONI SPECIFICHE

Le seguenti disposizione hanno valenza generale e vanno quindi applicate indipendentemente dallo strumento e/o dal trattamento dei dati preso in considerazione.

4.1. Uso delle apparecchiature

Sono da applicarsi le seguenti regole:

- Fatta eccezione per i telefoni cellulari e smartphone degli istruttori e dei dipendenti, in nessun caso l'incaricato dovrà utilizzare per il trattamento dei dati aziendali,

apparecchiature diverse da quelle di proprietà dell'azienda e fornite all'incaricato stesso al fine di adempiere alle mansioni affidategli;

- L'incaricato è tenuto a utilizzare gli strumenti informatici che l'azienda mette a sua disposizione solo per il trattamento di dati, documenti, files, programmi con finalità attinenti alle mansioni affidategli all'interno dell'azienda;
- Non sono quindi consentiti il trattamento (inteso come creazione, modifica, salvataggio, consultazione, ecc.), la trasmissione e/o la stampa di materiale che abbia contenuti non connessi con l'attività dell'azienda ed in ogni caso, qualsiasi informazione che possa ricadere in qualcuna delle seguenti categorie che vengono riportate a titolo esemplificativo ma non esaustivo:
    - materiale che abbia riferimenti o attinenze con l'aspetto politico e/o religioso;
    - materiale che sia riconducibile ad attività di tipo personale condotte a qualsiasi titolo, anche a non a scopo di lucro;
    - materiale ludico e/o di intrattenimento (giochi, utilities, sfondi colorati, fotografie, immagini, ecc.) non riconducibile all'attività svolta dall'incaricato con riferimento alle mansioni affidategli;
    - materiale con contenuti contrari al comune senso del pudore, pornografia, pedofilia, ecc.;
    - materiale soggetto alla legislazione nazionale ed internazionale sul diritto d'autore, sulla proprietà intellettuale, sui brevetti, ecc.
- E' fatto divieto di utilizzare gli strumenti forniti dall'azienda per mostrare e/o trasmettere, all'esterno dell'azienda, dati sensibili ai fini privacy e/o riservati con riferimento alle attività e alla strategia aziendali;
- E' fatto divieto utilizzare PC o strumenti non autorizzati dall'azienda per il trattamento dei dati (salvo gli smartphone dei dipendenti e degli istruttori).

4.2. Uso di PDA Personali / Smartphone

E' consentito ai istruttori e ai dipendenti l'uso di notebook e Smartphone non di proprietà dell'azienda per il trattamento di dati della struttura. In nessun caso l'utente dovrà comunque memorizzare su dispositivi non di proprietà dell'azienda, per tempo superiore al necessario, dati relativi all'attività dell'azienda stessa anche attraverso lo scambio via protocolli wireless come Bluetooth o similari.

4.3. Internet

E' fatto divieto agli incaricati al trattamento di utilizzare PdL forniti dall'azienda per:

- navigare in siti non attinenti allo svolgimento delle proprie mansioni; è tollerato l'utilizzo saltuario e personale di Internet, ferma restando la responsabilità del singolo incaricato e la facoltà dell'azienda di esercitare controlli;
- navigare su siti che presentino contenuti a sfondo sessuale, pornografico e pedopornografico,

- partecipare, per motivi non professionali e non attinenti allo svolgimento delle proprie mansioni a forum, chat-line, trading on-line, blog, sondaggi, ecc.;
- svolgere attività che influenzino negativamente la regolare operatività della rete dell'azienda o ne alterino l'utilizzabilità;
- è tollerato l'utilizzo saltuario e personale di Internet e l'utilizzo di sistemi di comunicazione diversi da quelli forniti dall'IT dell'azienda; questo vale sia per i collegamenti verso l'esterno, sia per i servizi di messaggistica immediata (Skype, MSN Messenger, AOL Messenger, ICQ o similari), in quanto sono potenziali veicoli di intrusione o di diffusione di informazioni riservate. Qualora il servizio di messaggistica immediata dovesse essere ritenuto utile dal punto di vista dell'azienda, verrà fornito uno strumento apposito, gestito dall'IT dell'azienda.
- registrarsi a siti i cui contenuti non siano legati all'attività lavorativa;
- scaricare files, anche su supporti magnetici/ottici, non aventi alcuna attinenza con le mansioni assegnate;
- utilizzare programmi e/o files audio o video non consoni con le mansioni ed i compiti assegnati;
- effettuare il download da Internet di materiale protetto da copyright o dalla legge sul diritto d'autore; qualora sulla rete aziendale o sui dischi fissi locali dei singoli PC / Pdl vengano individuati file di questo tipo si procederà d'ufficio alla loro rimozione;
- redigere, copiare, memorizzare, trasmettere documenti informatici di natura discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale o politica o di natura oltraggiosa, diffamatorio, oscena, ingiuriosa o altrimenti offensiva o illecita;
- Accedere a siti di social network come per esempio www.facebook.com, www.live.it, www.twitter.com, ecc.

Le suddette disposizioni si applicano alla navigazione Internet sia che venga effettuata tramite computer desktop o laptop piuttosto che attraverso Smartphone di proprietà dell'azienda e/o messi a disposizione degli incaricati dell'azienda.

4.4. Posta elettronica

L'utilizzo a fini personali della casella di posta elettronica dell'azienda è assolutamente vietato, salvo deroghe specifiche e autorizzate direttamente dagli amministratori, su indicazione del Responsabile di funzione al quale l'incaricato risponde gerarchicamente. Analogamente l'utilizzo della posta elettronica su palmari è da utilizzarsi solo a fini professionali.

5. REGOLAMENTO PER IL CORRETTO UTILIZZO DEGLI STRUMENTI ELETTRONICI

5.1. Accesso alla Pdl

Per accedere alle informazioni ed ai servizi del sistema informativo, l'incaricato deve fornire le proprie credenziali di accesso (user id e password) e provvedere all'esecuzione della procedura di accesso (log on). E' fatto obbligo di disconnettersi (log off) al termine dell'orario di lavoro e di bloccare la PdL (vedi in seguito) in caso di assenze anche brevi.

Le credenziali di accesso alla Pdl sono fornite all'incaricato dalla funzione IT e sono da considerarsi informazioni riservate e da trattarsi conseguentemente con le necessarie cautele.

- Alla prima assegnazione, l'incaricato - non appena effettuata l'autenticazione - dovrà provvedere a sostituire la password con una che risponda ai requisiti minimi di lunghezza minima 8 caratteri;
- non deve contenere riferimenti agevolmente riconducibili all'incaricato (es.: cognome, nome, codice di accesso, user id, data di nascita, riferimenti facilmente riconducibili a familiari, ecc.), 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 essere comunicata ad altri utenti;
- deve essere sostituita con la frequenza prevista dalle politiche di sicurezza dell'azienda, in ogni caso nel rispetto delle disposizioni di legge che prevedono l'obbligo di sostituzione almeno ogni sei mesi in caso di trattamento di dati comuni ed almeno ogni tre mesi in caso di trattamento di dati sensibili;
- in caso si richieda il ripristino della password, per diverse motivazioni, l'utente dovrà cambiarla subito dopo.

La password è personale ed é strettamente riservata. Conseguentemente non deve essere divulgata ad alcuno (ivi compresi personale interno e/o esterno ovvero terzi). Nel caso l'incaricato abbia anche solo il sospetto che altri incaricati ne siano venuti a conoscenza, dovrà attivarsi per cambiarla avvisando la funzione IT del possibile rischio di intrusione non autorizzata.

5.2. Accesso alla Pdl per attività di help desk

L'accesso alla PdL per attività di help desk è ammesso previo consenso dell'incaricato e preavviso. Il personale IT della società esterna è stato espressamente nominato ed autorizzato ad eseguire le suddette attività.

Non sono previste attività per il salvataggio dei dati contenuti sulle Pdl (drive locali quali C:\) e desktop. E' responsabilità dell'utente memorizzare i dati di pertinenza dell'azienda nelle apposite aree disco comuni appositamente predisposte dall'IT.

5.3. Blocco temporaneo della Pdl

Dopo un predeterminato periodo di inattività (massimo 10 minuti) la Pdl provvede automaticamente ad entrare in uno stato di blocco dal quale può essere fatta uscire solo dall'incaricato attraverso la digitazione delle proprie credenziali di accesso (user id e password).

5.4. Utilizzo della Pdl

L'incaricato dovrà agire con la massima diligenza e con tutti i mezzi a sua disposizione al fine di preservare la sicurezza del patrimonio dati dell'azienda.
L'incaricato dovrà farsi carico di ridurre il dispendio di risorse (carta, toner, fotocopie, ecc.) dovuto a incorretto utilizzo delle apparecchiature. Per esempio, dovrà evitare di:

- stampare documenti non necessari;
- utilizzare applicazioni grafiche se non necessario;
- utilizzare internet se non necessario;
- spedire allegati di grandi dimensioni;
- utilizzare risorse aziendali per fini personali.

E' espressamente vietato all'incaricato di intervenire sulla Pdl modificando la configurazione della stessa (software e/o hardware). Ogni intervento di modifica dovrà essere richiesto a un amministratore che interesserà la funzione IT, la quale – se del caso - provvederà a realizzarlo qualora necessario e in accordo con gli standard dell'azienda.

5.5. Password

<u>Comportamenti consigliati</u>

- scegliere una password difficile! Che la password contenga almeno dei numeri e/o dei segni di interpunzione e sia di lunghezza per legge non inferiore agli 8 caratteri;
- cambiare la password in accordo con gli standard dell'azienda (modificarla almeno ogni 6 mesi);
- tenere la password segreta e non diffonderla con nessun mezzo.

<u>Comportamenti vietati</u>

- scrivere la password su taccuini o foglietti;
- utilizzare le stesse credenziali di accesso al sistema informativo dell'azienda, ed in particolare la password, per l'accesso a servizi "pubblici" (es.: hotmail, libero, tiscali, ecc.).

5.6. Posta elettronica

Il sistema di posta elettronica (e-mail) dell'azienda è un servizio che permette agli utenti del sistema informativo di scambiarsi messaggi e allegati. Per allegati si intende qualsiasi file che può essere prodotto con uno dei software presenti nella dotazione

standard della PdI aziendale. In funzione delle mansioni ricoperte in azienda, vengono assegnate ai vari incaricati delle caselle postali dell'azienda.

5.7. Gestione della casella postale

La casella postale dell'incaricato è personale e deve essere accessibile solo fornendo le credenziali dello stesso. Per nessuna ragione la casella postale deve essere utilizzata da un incaricato diverso, salvo esplicita richiesta dello stesso di delegare l'accesso a personale di segreteria ovvero per necessità professionali o che per particolari esigenze gestionali rendano necessario ed urgente l'accesso da parte di altri incaricati ovvero in caso di assenza prolungata dello stesso incaricato assegnatario.
Le deleghe di accesso alla casella postale vanno richieste mediante notifica e-mail a un amministratore che, a sua volta, provvederà ad autorizzare la funzione IT.
Poiché potrebbero rendersi necessari detti accessi in assenza dell'assegnatario della casella di posta elettronica, accessi giustificati e legittimi alla luce del fatto che detta casella è un bene dell'azienda strumentale, messo a disposizione al singolo incaricato, dall'azienda in accordo con le funzioni assegnate allo stesso, l'azienda non potrà in nessun caso ritenersi responsabile qualora, in tale frangente, dovessero divenire pubbliche informazioni riservate e personali inerenti l'incaricato stesso.
<u>Comportamenti consigliati</u>

- In caso di assenza l'utente dovrà utilizzare la funzione "Fuori Sede" o "Out of Office". In caso di assenza prolungata (malattia, maternità, ferie, ecc.) inserire nel messaggio che notifica il "Fuori Sede", il nominativo e i recapiti dei colleghi cui i mittenti possono rivolgersi per avere pronta risposta. Esempio: "*Sono momentaneamente assente. La Vs. email verrà presa in considerazione al mio rientro. In caso di urgenza contattare XXXXXXXX (email: XXXXXXXXX)*".
- In fondo al messaggio di posta aggiungere sempre, in accordo con le disposizioni aziendali in materia, i dati come indicato nell'esempio seguente :
    - Nome e Cognome, Job Title, Indirizzo, Città, Telefono, Cellulare aziendale (se assegnato), Indirizzo email
- Non comunicare a destinatari poco affidabili o non conosciuti informazioni riguardanti l'azienda.
- Per ogni comunicazione cercare di utilizzare un singolo messaggio per raggiungere tutti i destinatari interessati. Allo stesso tempo però è consigliabile spedire messaggi a non più di una decina di destinatari alla volta.
- Assicurarsi di utilizzare la funzione "non-disclosure-recipient" (o CCN – Copia Carbone Nascosta) per i comunicati marketing e commerciale e comunque per gli invii a un numero rilevante di destinatari.
- La funzione "inoltra messaggio" altrui va fatta ad altri destinatari solo mettendo in copia conoscenza (cc) il mittente originale.
- Non spedire allegati superiori a 10 MB.
- Utilizzare la funzione copia per conoscenza (cc) solo se necessario e coinvolgendo solo i destinatari realmente interessati.

- Nell'oggetto della e-mail essere sintetici in modo che il destinatario capisca subito cosa fare del messaggio.
- Nell'oggetto della e-mail evitare di fare riferimento a persone.
- Utilizzare gli allegati solo se strettamente necessario.
- Nel caso di allegati di grandi dimensioni, utilizzare i programmi di compressione (ad es. WIN ZIP) per ridurli.
- In caso di ricezione di un file di tipo eseguibile (.exe) non aprirlo senza prima aver consultato la funzione IT.

Comportamenti sconsigliati

- Rispondere alle "catene di S. Antonio".
- Cancellare i messaggi prima ancora di averli letti, salvo che la provenienza sia dubbia. In questo caso, per evitare il contagio da possibili virus, cancellare l'email.
- Aprire messaggi che provengono da mittenti sconosciuti e/o aventi contenuti dubbi o discutibili.
- Utilizzare la posta elettronica per esprimere punti di vista ufficiali dell'azienda a meno che si sia stati a ciò espressamente autorizzati.
- Utilizzare la posta elettronica per spedire informazioni riservate (listini, prezzi, statistiche, dati di mercato, struttura organizzativa dell'azienda, ecc.) salvo nei casi previsti. Se dette informazioni devono essere inviate verso l'esterno, è opportuno ottenere la preventiva autorizzazione del Titolare.
- Abusare delle funzionalità che qualificano un messaggio come urgente, se non per reali necessità.
- Abusare delle funzionalità di ricevuta di ritorno e ricevuta di avvenuta lettura se non necessario: si consumano risorse dei server centrali e della rete locale dell'azienda.

5.8. Rubrica Personale

E' vietato utilizzare la rubrica del sistema di posta elettronica dell'azienda per memorizzare indirizzi di posta personali.

5.9. Utilizzo di supporti magnetici

Oggetti rimuovibili atti alla memorizzazione dei dati di uso corrente sono: dischetti, nastri, CD, memorie UBS ed altro.

I supporti rimovibili contenenti dati sensibili se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

I supporti magnetici contenenti dati sensibili devono essere custoditi in un'area ad accesso controllato o in un ufficio che è chiuso quando non presidiato o in archivi (armadio/cassetto) chiusi a chiave.

Non è consentito scaricare files contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa.
Tutti i files di provenienza incerta od esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo ed alla relativa autorizzazione all'utilizzo da parte dell'Amministratore del Sistema.
Non è consentito l'utilizzo di memorie usb, cd rom, cd riscrivibili, nastri magnetici o altri dispositivi di provenienza ignota.

6. MISURE DI SICUREZZA

L'azienda ha la responsabilità di proteggere il proprio patrimonio dati e tutelarsi da comportamenti lesivi e/o dannosi.
Ai fini del mantenimento del suddetto livello di sicurezza sono intraprese alcune specifiche attività di controllo e monitoraggio qui di seguito elencate.

6.1. Internet

Sono applicate le seguenti misure di sicurezza e controllo:

- L'azienda si riserva la facoltà di oscurare o impedire l'accesso ai siti che possono compromettere la sicurezza delle connessioni e dei servizi che risultano in violazione della legislazione italiana e comunitaria vigente;
- al fine di garantire adeguata sicurezza al patrimonio dei dati dell'azienda, e anche al fine di ovviare alle situazioni di pericolo e/o rischio derivanti da attacchi ai sistemi informativi, tutti gli accessi ad Internet sono soggetti a monitoraggio da parte del Titolare. Gli accessi sono memorizzati in archivi elettronici che risultano essere:
    - soggetti a cancellazione periodica automatica da parte del software di controllo con cadenza trimestrale;
    - non accessibili al personale interno della LAN dell'azienda;
    - disponibili alle autorità competenti (Guardia di Finanza, Polizia, Carabinieri, Autorità Giudiziaria, Ispettori del Garante, ect.) in caso di indagini e/o richieste specifiche.

6.2. Posta elettronica

- La casella postale dell'azienda viene eliminata all'atto della cessazione del rapporto tra dipendente o collaboratore e azienda (vedi procedura nel paragrafo seguente).
- Il sistema di posta elettronica dell'azienda viene protetto da sistemi automatici di controllo che provvedono a rifiutare messaggi di posta elettronica provenienti da siti ritenuti, dal sistema di controllo, dubbi e/o considerati generatori di mail inutili e/o dannose (spam).

- Il blocco viene attivato automaticamente su tutte le caselle postali dell'azienda ed è operativo a partire dalle segnalazioni provenienti dai sistemi di controllo internazionali fornite dai vari provider Internet.
- Nel caso l'incaricato sospetti che un messaggio di posta elettronica a lui inviato non sia stato ricevuto, deve provvedere ad avvisare il Titolare indicando l'indirizzo di posta elettronica completo del mittente.
- Le caselle postali "di funzione" sono rese disponibili per necessità organizzative legate all'esigenza di permettere a più incaricati di operare sulla stessa casella postale. La casella postale di funzione possiede quindi un indirizzo di posta elettronica che ne esemplifica al mittente la funzionalità (es.: info@atleticapbm.it). Attualmente esistono 3 caselle di posta elettronica di funzione:

Casella	Viene letta da
info@atleticapbm.it	1 consigliere e 1 addetta
cmsbovisio@atleticapbm.it	2 consiglieri e 1 addetta
segreteria@atleticapbm.it	1 consigliere e 1 addetta

6.3. Utilizzo di archivi cartacei contenenti dati sensibili

Specifiche istruzioni sono fornite agli incaricati della Direzione del Personale per garantire adeguata sicurezza di trattamento dei dati sensibili del personale dipendente.
In particolare per quanto riguarda i supporti cartacei:

- i curricula di potenziali collaboratori/istruttori/dipendenti devono essere conservati nell'ufficio amministrazione, in un armadio chiuso a chiave. In caso di curricula utilizzati all'esterno dell'ufficio precedentemente indicato questi documenti devono essere riposti nel luogo prescritto subito dopo il loro utilizzo.
- i dati cartacei relativi alle presenze dei dipendenti devono essere conservati all'interno dell'ufficio amministrazione, in un armadio chiuso a chiave. In caso di utilizzo dei documenti all'esterno dell'ufficio precedentemente indicato, questi devono essere riposti nel luogo prescritto subito dopo il loro utilizzo.
- i dati cartacei relativi ai cedolini paga, alle malattie e in generale alle informazioni necessarie per la gestione delle retribuzioni e dei rapporti di lavoro devono essere conservati all'interno dell'ufficio amministrazione, in appositi archivi siti in armadi chiusi a chiave. In caso di utilizzo dei documenti all'esterno dell'ufficio precedentemente indicato questi documenti devono essere riposti nel luogo prescritto subito dopo il loro utilizzo.
- i dati e la documentazione relativi agli adempimenti di cui al D.Lgs. 81/2008 sono conservati nell'ufficio amministrazione, in un apposito archivio conservato in un armadio chiuso a chiave. In caso di utilizzo dei documenti all'esterno dell'ufficio precedentemente indicato, questi documenti devono essere riposti nel luogo prescritto subito dopo il loro utilizzo.
- i dati cartacei relativi a clienti e fornitori devono essere conservati all'interno dell'ufficio amministrazione, dell'ufficio commerciale e dell'ufficio magazzino in appositi archivi conservati in armadi chiusi a chiave. In caso di utilizzo dei

documenti all'esterno degli uffici precedentemente indicati questi documenti devono essere riposti nei luoghi prescritti subito dopo il loro utilizzo.

- ogni volta che le persone incaricate del trattamento dei dati lasciano gli uffici della Società devono chiudere la porta a chiave, dopo aver riposto i documenti negli appositi cassetti/armadi.
- ogni volta che si raccolgono dati personali è necessario rilasciare l'informativa del caso all'interessato.
- non comunicare dati a persone non autorizzate.