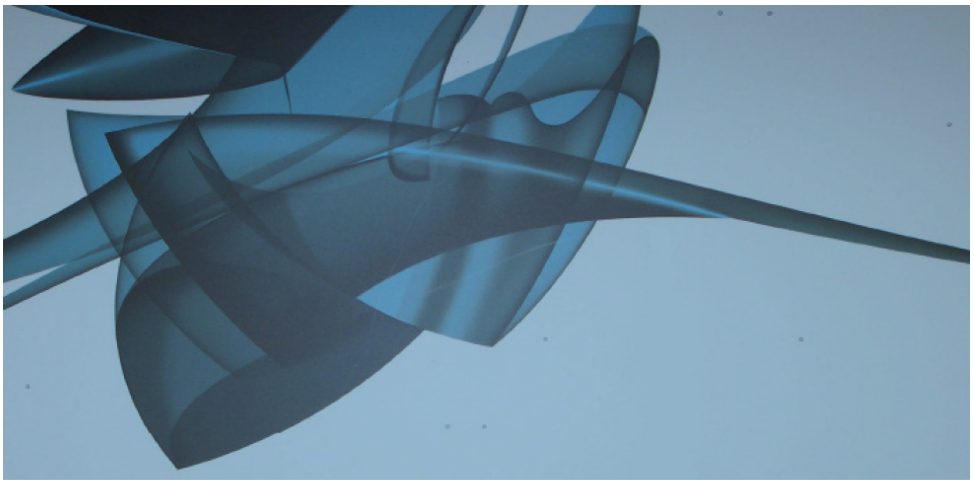
CONSORZIO PER LO SVILUPPO INDUSTRIALE DEL COMUNE DI MONFALCONE (C.S.I.M.)



Modello Organizzativo ai sensi del D.Lgs. 231/2001

Parte Speciale D Reati informatici e trattamento illecito di dati

Rev.	Oggetto	Approvazione	Data
00	Modello di Organizzazione Gestione e Controllo ex D.Lgs. 231/01 – Parte Speciale D	CdA	02.02.2012
01	Aggiornamento	CdA	18.12.2015

Sommario

1. PARTE SPECIALE D 3
1.1 Premessa 3
2. DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI 4
2.1 Accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.) 4
2.2 Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quarter c.p.) 4
2.3 Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.) 4
2.5 Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.) 5
2.6 Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.) 5
2.7 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.) 5
2.8 Danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.) 5
2.9 Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.) .. 5
2.10 Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies c.p.) 6
2.11 Documenti informatici (art. 491 bis c.p.) 6
3. MAPPATURA DEI RISCHI 7
3.1 Introduzione 7
3.2 Definizioni 7
3.3 Attività a rischio o sensibili 8
3.4 Analisi dei trattamenti informatici eseguiti dal CSIM 8
4. PROCEDURE PREVENTIVE ADOTTATE DAL CSIM 9
4.1 Sistema di autenticazione e autorizzazione 9
4.2 Procedure di salvataggio e di continuità 9
4.3 Conservazione e sostituzione dei supporti 9
4.4 Protezione antivirus 9
4.5 Aggiornamento dei software 9
4.6 Formazione del Personale 9
4.7 Documento Programmatico sulla Sicurezza 10
5. PRINCIPI GENERALI DI COMPORTAMENTO 11
6. CONTROLLI DELL'ORGANISMO DI VIGILANZA 12

1. PARTE SPECIALE D

1.1 Premessa

La legge 18 marzo 2008, n. 48 recante "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno" ha inserito nel D.Lgs. n. 231/2001 l'**articolo 24 bis**, così estendendo la responsabilità amministrativa degli enti anche a **"Delitti informatici e trattamento illecito di dati"**.

Le sanzioni sono sia pecuniarie (da cento a cinquecento quote), sia interdittive previste dall'art. 9, comma 2, del D.lgs. 231/2001. In particolare la norma in esame stabilisce che:

- 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. Nei casi di condanna per uno dei delitti indicati si applicano le sanzioni interdittive di cui all'art. 9, comma 2, lettere a), b) ed e) del D.lgs. 231/2001.
- 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. Nei casi di condanna per uno dei delitti indicati si applicano le sanzioni interdittive di cui all'art. 9, comma 2, lettere b) ed e) del D.lgs. 231/2001.
- 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 D.lgs. 231/2001 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. Nei casi di condanna per uno dei delitti indicati si applicano le sanzioni interdittive di cui all'art. 9, comma 2, lettere c), d) ed e) del D.lgs. 231/2001.

Nei paragrafi seguenti vengono analizzate le fattispecie delittuose previste dall' art. 24 bis del D.Lgs. 231/2001.

2. DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

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

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

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

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

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 € 5.164,00.
La pena è della reclusione da uno a due anni e della multa da € 5.164,00 a € 10.329,00 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater

2.3 Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.)

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 € 10.329,00.

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

Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da 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 comunicazioni di cui al primo comma.

I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.
Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso: 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; 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; da chi esercita anche abusivamente la professione di investigatore privato.

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

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.
La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater.

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

Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre 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 della reclusione da uno a quattro anni e si procede d'ufficio.

2.7 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.)

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.
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.

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

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

2.9 Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.)

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.

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.

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

Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da € 51,00 a € 1.032,00.

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

Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private.

3. MAPPATURA DEI RISCHI

3.1 Introduzione

La presente parte ha l'obiettivo di illustrare i criteri, le responsabilità e le norme comportamentali a cui tutti i Destinatari a qualsiasi titolo del Consorzio devono attenersi nella gestione dei rapporti e degli adempimenti verso la Pubblica Amministrazione e le Autorità pubbliche di Vigilanza, per evitare la commissione dei reati previsti dall'art. 24 bis del D.lgs 231/2001 ed agire nel rispetto dei principi di massima trasparenza, tempestività e tracciabilità delle attività svolte.
Nello specifico, il presente Allegato ha lo scopo di:

1. definire le procedure che tutti i Destinatari del CSIM devono osservare al fine di applicare correttamente le prescrizioni contenute nei documenti del Modello 231;
2. supportare l'Organismo di Vigilanza nell'espletamento delle attività di controllo, monitoraggio e verifica.

3.2 Definizioni

- Credenziali: l'insieme degli elementi identificativi di un utente o di un account (generalmente UserID e Password).

- Dati Informatici: qualunque rappresentazione di fatti, informazioni, o concetti in forma idonea per l'elaborazione con un sistema informatico, incluso un programma in grado di consentire ad un sistema informatico di svolgere una funzione.

- Documento/i Informatico/i: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

- Firma Elettronica: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.

- Password: sequenza di caratteri alfanumerici o speciali necessaria per autenticarsi ad un sistema informatico o ad un programma applicativo.

- Piano di Sicurezza: documento che definisce un insieme di attività coordinate che devono essere intraprese per implementare la politica di sicurezza del sistema.

- Postazione di Lavoro: postazione informatica aziendale fissa oppure mobile in grado di trattare informazioni aziendali.

- Sicurezza Informatica: l'insieme delle misure organizzative, operative e tecnologiche finalizzate a salvaguardare i trattamenti delle informazioni effettuati mediante strumenti elettronici.

- Sistemi Informativi: l'insieme della rete, dei sistemi, dei data base e delle applicazioni aziendali.

- Spamming: invio di numerosi messaggi indesiderati, di regola attuato attraverso l'utilizzo della posta elettronica.

- Virus: programma creato a scopo di sabotaggio o vandalismo, in grado di alterare il funzionamento di risorse informatiche, di distruggere i dati memorizzati, nonché di propagarsi tramite supporti rimovibili o reti di comunicazione.

3.3 Attività a rischio o sensibili

In relazione ai reati e alle condotte criminose previste dall'art. 24 bis del D.Lgs. 231/2001, le aree ritenute più specificamente a rischio risultano essere, ai fini della presente Parte Speciale del Modello, le seguenti:

- tutte le attività aziendali svolte dai Destinatari tramite l'utilizzo dei Sistemi Informativi aziendali, del servizio di posta elettronica e dell'accesso ad Internet;
- gestione dei Sistemi Informativi aziendali al fine di assicurarne il funzionamento e la manutenzione;
- gestione dei flussi informativi elettronici con la pubblica amministrazione.

3.4 Analisi dei trattamenti informatici eseguiti dal CSIM

<table>
<tr><th>Attività svolta</th><th>Soggetti coinvolti</th><th>Funzioni responsabili</th><th>Ipotesi di reato</th></tr>
<tr><td>Corrispondenza in entrata e in uscita</td><td>Aziende Soggetti pubblici e privati</td><td>Ufficio Direzione/ Amministrativo</td><td rowspan="7">Accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.)- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quarter c.p.)- Dfusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.)- Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.)-Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.)- 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.)- Danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.)- Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.)- Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies c.p.) modificare un documento informatico ad interesse o vantaggio dell'Ente.</td></tr>
<tr><td>Gestione fiscale ed economica</td><td>Clienti e fornitori</td><td>Ufficio Amministrativo</td></tr>
<tr><td>Gestione del personale</td><td>Dipendenti</td><td>Ufficio Amministrativo</td></tr>
<tr><td>Curricula vitae, richieste di assunzione o di inizio rapporto contrattuale</td><td>Soggetti privati</td><td>Ufficio Direzione /Amministrativo</td></tr>
<tr><td>Gestione aziende insediate nelle aree industriali</td><td>Aziende insediate</td><td>Ufficio Direzione /Amministrativo</td></tr>
<tr><td>Provvedimenti, anagrafiche e corrispondenza organi societari</td><td>Soci</td><td>Ufficio Direzione /Amministrativo</td></tr>
<tr><td>Gestione clienti e fornitori</td><td>Clienti e fornitori</td><td>Ufficio Direzione /Amministrativo</td></tr>
<tr><td colspan="3">Modalità di commissione</td></tr>
<tr><td colspan="3">- Soggetti si procurano codici di accesso ai sistemi informatici al fine di accedere al sistema interno ed effettuare operazioni che portino interesse o vantaggio per il Consorzio.
- Soggetti si procurano codici di accesso di sistemi informatici al fine di accedere a sistemi esterni e procurare un interesse o vantaggio all'Ente
- Soggetti che si introducono nel sistema informatico dell'Ente per effettuare operazioni che portino un interesse o vantaggio per l'Ente (diminuzione del credito dei clienti,maggiorazione dei costi, falsificazione fatture).</td></tr>
</table>

4. PROCEDURE PREVENTIVE ADOTTATE DAL CSIM

4.1 Sistema di autenticazione e autorizzazione

L'accesso in rete è subordinato ad una procedura obbligatoria di login con impiego di password personale a seguito della quale l'utente viene autenticato dal controllore del Dominio (PDC).
Agli utenti corrispondono password non conosciute neanche all'amministratore di sistema. Gli utenti sono organizzati in gruppi rispetto ai quali sono definiti il livello e la tipologia di risorse a cui possono accedere attraverso determinati profili.
Detti profili possono essere attivati, modificati, revocati dall'amministratore del sistema su precisa indicazione dell'Ente.
Sono state impartite adeguate disposizioni agli utenti in merito all'utilizzo delle password ed ai criteri legati alla sicurezza delle stesse.
A tal fine va chiarito che proprio la definizione di utenti, gruppi ed abilitazioni sulle diverse condivisioni consentono un alto livello di sicurezza sui server, garantendo che un utente appartenente ad un gruppo diverso non potrà mai vedere od alterare dati su di una condivisione che non gli spetta.

4.2 Procedure di salvataggio e di continuità

I dati memorizzati su server sono soggetti a backup settimanale completo e giornaliero incrementale su base storica mensile consentendo quindi un recupero degli stessi fino a 5 settimane lavorative precedenti un possibile incidente. Anche il sistem-status è soggetto a backup su base settimanale. Il server è dotato di sistema di dischi ridondanti hot-swap configurati RAID 5 a garanzia della continuità di servizio in caso di guasto di uno di essi. Il server è supportato da sistema di alimentazione ridondante e da connessione di rete su doppia scheda per funzionalità di load-balancing e di failover.

4.3 Conservazione e sostituzione dei supporti

Le procedure di backup vengono eseguite giornalmente su dispositivo di rete NAS indipendente. Periodicamente viene eseguita una verifica a campione dei backup effettuati o comunque, in caso di malfunzionamento, viene effettuata una verifica sistematica delle registrazioni.

4.4 Protezione antivirus

Sia il server che tutte le postazioni client sono dotate di sistema antivirus. L'aggiornamento delle impronte virali viene fatto in maniera sistematica di norma con periodicità quotidiana ma, in momenti particolari, anche più volte nell'arco delle 24 ore.
La rete locale è dotata di protezione perimetrale in quanto collegata alla rete internet per mezzo di un firewall e di un modem-router ADSL.

4.5 Aggiornamento dei software

Tutti i software di impiego generale e condiviso (antivirus, browser internet, proxy, office automation, ecc.) vengono costantemente aggiornati appena disponibili patch scaricabili dai relativi siti. Particolare riguardo è dedicato alle "security patch" legate ai programmi di navigazione o comunque relazionati al mondo internet.

4.6 Formazione del Personale

Sono previsti incontri formativi di aggiornamento per il personale incaricato con professionisti in merito sia alle tematiche giuridico che tecniche, sulle problematiche inerenti al trattamento dei dati, per informarli ed

aggiornarli dei rischi che incombono sul trattamento, sulle misure disponibili per prevenire eventi dannosi, sui profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, sulle responsabilità che ne derivano e sulle modalità per aggiornarsi alle misure minime adottate dal titolare.
I dipendenti, neo assunti, o in caso di cambiamento di mansioni, effettueranno degli incontri formativi sulle modalità di trattamento dei dati e del relativo protocollo di sicurezza con i responsabili di Servizio e con il consulente informatico. Analoghi interventi formativi sono previsti in caso di introduzione di nuovi strumenti per il trattamento dei dati.

4.7 Documento Programmatico sulla Sicurezza

È prevista l'aggiornamento annuale del Documento Programmatico sulla Sicurezza (DPS). In questo documento sono analizzate le situazioni aziendali ed organizzate le procedure a garanzia della sicurezza nei trattamenti dei dati. In particolare:
Gestione e monitoraggio degli accessi ai sistemi informatici e telematici, nell'ambito della quale sono ricomprese le attività di:

- gestione del profilo utente e del processo di autenticazione
- gestione e protezione della postazione di lavoro
- gestione degli accessi verso l'esterno
- gestione e protezione delle reti
- gestione degli output di sistema e dei dispositivi di memorizzazione
- Sicurezza fisica

5. PRINCIPI GENERALI DI COMPORTAMENTO

- E' vietato connettere ai sistemi informatici del CSIM personal computer, periferiche, altre apparecchiature o installare software senza preventiva autorizzazione;
- è vietato in qualunque modo modificare la configurazione software e/o hardware di postazioni di lavoro fisse o mobili se non previsto da una regola aziendale ovvero, in diversa ipotesi, se non previa espressa autorizzazione;
- è vietato divulgare, cedere o condividere con personale interno o esterno al Consorzio le proprie Credenziali di accesso ai sistemi e alla rete informatica
- è vietato accedere abusivamente ad un sistema informatico altrui – ovvero nella disponibilità di altri Dipendenti o terzi – nonché accedervi al fine di manomettere o alterare abusivamente qualsiasi dato ivi contenuto;
- è vietato manomettere, sottrarre o distruggere il patrimonio informatico del Consorzio o di terze parti, comprensivo di archivi, dati e programmi;
- è vietato sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici del Consorzio o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi;
- è vietato comunicare a persone non autorizzate, interne esterne al CSIM, i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati;
- è proibito mascherare, oscurare o sostituire la propria identità e inviare e-mail riportanti false generalità o inviare intenzionalmente e-mail contenenti Virus o altri programmi in grado di danneggiare o intercettare dati.

IL CSIM si impegna, a sua volta, a porre in essere i seguenti adempimenti:

1) informare adeguatamente i Dipendenti dell'importanza di mantenere le proprie Credenziali confidenziali e di non divulgare le stesse a soggetti terzi;
2) prevedere attività di formazione e addestramento periodico in favore dei Dipendenti al fine di diffondere una chiara consapevolezza sui rischi derivanti da un utilizzo improprio delle risorse informatiche;
3) informare i Dipendenti della necessità di non lasciare incustoditi i propri sistemi informatici e di bloccarli, qualora si dovessero allontanare dalla Postazione di Lavoro, con i propri codici di accesso;
4) impostare le postazioni di lavoro in modo tale che, qualora non vengano utilizzati per un determinato periodo di tempo, si blocchino automaticamente;
5) limitare gli accessi alle stanze server unicamente al personale autorizzato;
6) dotare i sistemi informatici di adeguato software firewall e antivirus e far sì che, ove possibile, questi non possano venir disattivati;
7) prevedere un procedimento di autenticazione mediante l'utilizzo di Credenziali al quale corrisponda un profilo limitato della gestione di risorse di sistema, specifico per ognuno dei Dipendenti.

6. CONTROLLI DELL'ORGANISMO DI VIGILANZA

I compiti di vigilanza dell'OdV in relazione all'osservanza del Modello per quanto concerne i Reati di cui all'art. 24 bis del Decreto sono i seguenti:

- svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare periodicamente la loro efficacia a prevenire la commissione dei Reati di cui all'art. 24 bis. L'OdV, avvalendosi eventualmente della collaborazione di consulenti tecnici competenti in materia, condurrà una periodica attività di analisi sulla funzionalità del sistema preventivo adottato e proporrà ai soggetti competenti eventuali azioni migliorative o modifiche qualora vengano rilevate violazioni significative delle norme sui Delitti Informatici, ovvero in occasione di mutamenti nell'organizzazione aziendale e nell'attività in relazione al progresso scientifico e tecnologico;
- proporre e collaborare alla predisposizione delle istruzioni standardizzate relative ai comportamenti da seguire nell'ambito delle Aree a Rischio individuate nella presente Parte Speciale
- esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.