MODELLO ORGANIZZATIVO E GESTIONALE

(MOG)

D. Lgs. 8 giugno 2001, n. 231

Parte Speciale "F"

Reati informatici e trattamento illecito dei dati

Il presente elaborato e tutti gli allegati si intendono integrati con il Piano Triennale per la prevenzione della Corruzione e della Trasparenza 2020 - 2022.

Redatto dal Responsabile della Prevenzione alla Corruzione e della Trasparenza

Adottato in data 06.12.2019 con deliberazione Commissariale n. 429/19 del 06.12.2019

Pubblicato sul sito internet nella sezione "Amministrazione Trasparente in data 05.02.2020

Il Direttore Generale: firmato Dott. Vito Caputo

Il Commissario: firmato Dott. Alfredo Borzillo

Indice

Premessa

La presente Parte Speciale riguarda i reati previsti dagli artt. 24-bis e 25-novies del D.Lgs n. 231/01 ovvero i reati c.d. informatici e delitti in violazione del diritto di autore.

L'articolo relativo ai reati informatici è stato inserito dall'art. 7 della Legge 18 marzo 2008 n. 48 (Legge di ratifica della Convenzione del Consiglio di Europa anche conosciuta come Convenzione di Budapest del 23 novembre 2011).

Viceversa ai sensi dell'art. 15, comma 7 lett. C) della Legge 23 luglio 2009 n. 99 è configurabile a carico dell'ente la responsabilità amministrativa dipendente dalla realizzazione dei delitti in materia di violazione del diritto di autore elencati dall'art. 25-novies del D.lgs n. 231/01.

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."

Detenzione e diffusione abusive di codici di accesso a sistemi informatici o telematici (art. 615-quater 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 lire dieci milioni. 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. Il quarto comma dell'art. 617-quater c.p. prevede: - al n. 1 che l'azione sia eseguita 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 utilità; - al n. 2 che l'azione sia eseguita da un pubblico ufficiale o da un incaricato di pubblico servizio con abuso di poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore di sistema."

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

"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 o 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 € 10.329,00."

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

"Chiunque fraudolentamente 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:

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 od interrompere comunicazioni informatiche o telematiche (art. 617-quinques 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."

Danneggiamento di sistemi informatici e telematici (art. 635-bis c.p.)

"Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni. Se ricorre una o più delle circostanze di cui al 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."

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."

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."

Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 615-quinques 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."

Frode informatica del soggetto che presta servizio di certificazione di firma elettronica (art. 640-quinques c.p.)

"Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad

altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro".

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."

Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171, comma 1, abis, Legge 22 aprile 1941 n. 633)

"Salvo quanto previsto dall'art. 171-bis e dall'articolo 171-ter, è punito con la multa da € 51,00 a € 2.065,00 chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma: a-bis) mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa." Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171, comma 3, Legge 22 aprile 1941 n. 633).

La pena è della reclusione fino ad un anno o della multa non inferiore ad € 516,00 se i reati di cui sopra sono commessi sopra un'opera altrui non destinata alla pubblicazione, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore."

Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171-bis, Legge 22 aprile 1941 n. 633)

"Chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE), è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da € 2.582,99 a € 15.493,00. La stessa pena si applica se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori. La pena non è inferiore nel minimo a due anni di reclusione e la multa a € 15.493,00 se il fatto è di rilevante gravità.

Chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter, ovvero distribuisce, vende o concede in locazione una banca di dati, è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da € 2.582,99 a € 15.493,00. La pena non è inferiore nel minimo a due anni di reclusione e la multa ad € 15.493,00 se il fatto è di rilevante gravità."

Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171-ter, Legge 22 aprile 1941 n. 633)

"1. È punito, se il fatto è commesso per uso non personale, con la reclusione da sei mesi a tre anni e con la multa da euro 2.582 a euro 15.493 (da cinque a trenta milioni di lire) chiunque a fini di lucro:

a) abusivamente duplica, riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento;

b) abusivamente riproduce, trasmette o diffonde in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati;

c) pur non avendo concorso alla duplicazione o riproduzione, introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, pone in commercio, concede in noleggio o comunque cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della televisione con qualsiasi procedimento, trasmette a mezzo della radio, fa ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui alle lettere a) e b);

d) detiene per la vendita o la distribuzione, pone in commercio, vende, noleggia, cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale è prescritta, ai sensi della presente legge, l'apposizione di contrassegno da parte della Società italiana degli autori ed editori (SIAE), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato;

e) in assenza di accordo con il legittimo distributore, ritrasmette o diffonde con qualsiasi mezzo un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato;

f) introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, vende, concede in noleggio, cede a qualsiasi titolo, promuove commercialmente, installa dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto;

f-bis) fabbrica, importa, distribuisce, vende, noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti ovvero presta servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'articolo 102-quater ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure. Fra le misure tecnologiche sono comprese quelle applicate, o che residuano, a seguito della rimozione delle misure medesime conseguentemente a iniziativa volontaria dei titolari dei diritti o ad accordi tra questi ultimi e i beneficiari di eccezioni, ovvero a seguito di

esecuzione di provvedimenti dell'autorità amministrativa o giurisdizionale;

h) abusivamente rimuove o altera le informazioni elettroniche di cui all'articolo 102-quinquies, ovvero distribuisce, importa a fini di distribuzione, diffonde per radio o per televisione, comunica o mette a disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse.

2. È punito con la reclusione da uno a quattro anni e con la multa da euro 2.582 a euro 15.493 (cinque a trenta milioni di lire) chiunque:

a) riproduce, duplica, trasmette o diffonde abusivamente, vende o pone altrimenti in commercio, cede a qualsiasi titolo o importa abusivamente oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi;

a-bis) in violazione dell'articolo 16, a fini di lucro, comunica al pubblico immettendola in un sistema di reti telematiche, mediante concessioni di qualsiasi genere, un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa;

b) esercitando in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione, importazione di opere tutelate dal diritto d'autore e da diritti connessi, si rende colpevole dei fatti previsti dal comma 1;

c) promuove o organizza le attività illecite di cui al comma 1.

3. La pena è diminuita se il fatto è di particolare tenuità.

4. La condanna per uno dei reati previsti nel comma 1 comporta:

a) l'applicazione delle pene accessorie di cui agli articoli 30 e 32-bis del codice penale;

b) la pubblicazione della sentenza ai sensi dell'articolo 36 del codice penale;

c) la sospensione per un periodo di un anno della concessione o autorizzazione di diffusione radiotelevisiva per l'esercizio dell'attività produttiva o commerciale.

5. Gli importi derivanti dall'applicazione delle sanzioni pecuniarie previste dai precedenti commi sono versati all'Ente nazionale di previdenza ed assistenza per i pittori e scultori, musicisti, scrittori ed autori drammatici."

AREA A RISCHIO 1: ACCESSO A SISTEMI INFORMATICI/TELEMATICI DI ENTI PUBBLICI, CLIENTI E FORNITORI.

AREA A RISCHIO 2: ACCESSO ALLE INFORMAZIONI RELATIVE ALL'UTILIZZO DEI SISTEMI INFORMATIVI.

AREA A RISCHIO 3: PREDISPOSIZIONE E PUBBLICAZIONE DI COMUNICATI STAMPA O MATERIALE PROMOZIONALE.

AREA A RISCHIO 4: UTILIZZO DI SOFTWARE AZIENDALE NON LICENZIATO NEI COMPUTER DELL'ENTE.

PROTOCOLLO DI COMPORTAMENTO E DI PREVENZIONE

NORME DI COMPORTAMENTO

È imposto il divieto nei confronti del CDA/Commissario, della DG, dei dipendenti e dei collaboratori esterni del Consorzio di porre in essere, collaborare o dare causa alla realizzazione di comportamenti e/o fatti che, considerati individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato informatico previste dal D.lgs. n. 231/2001 sia nella forma consumata che nella forma tentata.

In particolare, è fatto **espresso divieto** di:

- tenere qualunque comportamento che, sebbene non appaia idoneo a costituire di per sé una o più fattispecie di reato informatico, possa potenzialmente realizzarlo;
- utilizzare informazioni, applicazioni ed apparecchiature informatiche per ragioni diverse rispetto a quelle lavorative;
- cedere o prestare a altri soggetti l'utilizzo delle apparecchiature informatiche in assenza di alcuna esigenza consortile giustificata;
- diffondere, utilizzare, copiare, trasferire, inoltrare files e/o documenti informatici e/o qualunque altra documentazione riservata nonché relativa all'attività del Consorzio salvo il caso in cui ciò si renda necessario per il conseguimento dell'oggetto sociale;
- lasciare non custodito il proprio PC senza averlo reso non accessibile agli altri operatori;
- utilizzare le credenziali di accesso al sistema informatico di altri soggetti, salvo previo loro espresso consenso e solo per ragioni di carattere lavorativo e mai personale;
- accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
- cancellare e/o alterare e/o manomettere e/o distruggere e/o dati, documenti, o informazioni informatici;
- detenere e/o diffondere e/o utilizzare abusivamente codici, parole chiave, o altri mezzi idonei all'accesso ad un sistema informatico o telematico al fine di acquisire informazioni riservate di concorrenti;
- alterare, cancellare, distruggere, falsificare documenti informatici ricevuti e/o disponibili sul server relativi all'attività gestionale dell'Ente;
- accedere abusivamente a sistemi interbancari;
- accedere abusivamente a sistemi dell'Ente protetti da misure di sicurezza al fine di attivare servizi non richiesti dal contribuente;
- detenere e utilizzare le credenziali di accesso alle caselle di posta e – mail dei dipendenti salvo che ciò si renda necessario al fine di acquisire informazioni relative all'attività svolta dal Consorzio e solo previo consenso del soggetto interessato;

- diffondere abusivamente numeri seriali di telefoni cellulari;
- danneggiare informazioni/dati aziendali/programmi aziendali infrastrutture tecnologiche/sistemi di conservazione dei documenti di soggetti concorrenti;
- danneggiare, distruggere, manomettere documenti probatori registrati presso gli enti pubblici o informazioni, dati e programmi informatici in uso alla PA;
- impedire o interrompere una comunicazione al fine di evitare che un concorrente trasmetta dati e/o l'offerta per la partecipazione di una gara;
- installare apparecchiature finalizzate ad intercettare ed impedire informazioni informatiche;
- non divulgare informazioni e/o dati e/o documenti riferiti a terzi e/o all'Ente verso l'esterno.

A tale fine, è fatto obbligo al CDA/Commissario, alla DG, ai dipendenti ed ai collaboratori esterni nei limiti di quanto previsto negli accordi sottoscritti con il Consorzio:

1. rispettare le regole di comportamento e i valori espressi nel Codice Etico dell'Ente;
2. comunicare all'Odv e/o al proprio Responsabile qualunque anomalia e/o comportamento sospetto di cui si è venuti a conoscenza nell'esercizio della propria attività lavorativa;
3. segnalare tempestivamente e senza indugio ogni anomalia e/o malfunzionamento e/o inoperatività riferita ai sistemi o programmi informatici al Responsabile dell'area informatica;
4. non accedere a sistemi informatici senza il consenso della persona autorizzata;
5. non accedere e/o utilizzare i sistemi o programmi informatici per usi diversi rispetto a quelli per i quali sono stati destinati e al fine di arrecare un danno a terzi o a imprese concorrenti.

STRUTTURA INFORMATICA

La Struttura del Sistema Informatico dell'Ente è suddivisa in:

- HARDWARE (HW) a cui appartengono i PC Client (desktop, Notebook, Tablet), i Server, le reti locali LAN (Local Area Network), stampanti, Reti di comunicazione, Supporti di memorizzazione;
- SOFTWARE (SW) di base a cui appartengono i sistemi operativi, i software per lo sviluppo di applicazioni e i SW applicativi a cui appartengono i software acquistati da terze parti o sviluppati all'interno dell'Ente ed utilizzati dagli utenti per gestire determinati processi consortili.

ARCHITETTURA RETE AZIENDALE

STRUTTURA HARDWARE

La rete interna dell'Ente è protetta attraverso un firewall perimetrale che consente di discriminare l'accesso a internet esterno.

L'accesso alla rete internet dagli utenti è consentita solo per l'esercizio dell'attività lavorativa.

Nei locali del Consorzio è presente una rete Wireless a cui possono accedere solo gli utenti espressamente autorizzati.

La configurazione base dei PC e la loro caratteristica tipologia di connessione è conservata presso il singolo operatore cui l'hardware è assegnato.

Le attività di assistenza e manutenzione HW sono valutate tenuto conto della singola situazione oggettiva a cui seguono le dovute misure scelte dal Dirigente dell'Area previa consultazione con la DG.

STRUTTURA SOFTWARE

I PC dell'Ente sono in possesso della configurazione SW base, conservata ed aggiornata dal singolo operatore cui l'hardware è assegnato.

Gli utenti non possono installare software anche gratuiti né installare dispositivi di memorizzazione, comunicazione o di altra natura (quali, a titolo esemplificativo ma non esaustivo, modem, masterizzatori).

Le azioni di variazione della configurazione base dei SW presenti sui PC e Server sono aggiornamenti del SW e l'installazione di patch di sicurezza (correzioni del SW).

Ogni PC è dotato di procedure di controllo per l'installazione di software sui sistemi operativi e di programmi di protezione da attacchi esterni tramite antivirus e filtro in uscita tramite proxy. Qualora il software antivirus rilevi la presenza di un virus nel sistema, l'utente interessato dovrà immediatamente sospendere ogni attività in corso senza spegnere il PC e segnalare l'accaduto al Dirigente dell'Area.

Ogni dispositivo esterno dovrà essere sottoposto al controllo antivirus prima di essere utilizzato e qualora venga rilevato un virus, il dispositivo dovrà essere sottoposto ad opportune verifiche. Tutti i file contenenti software o eseguibili dovranno essere controllati e contrassegnati come esenti da virus prima della consegna a terzi.

GESTIONE DEGLI UTENTI INFORMATICI

La sicurezza all'accesso delle informazioni è garantita dall'autenticazione: ogni utente possiede ID e PSW che gli viene attribuito previa disposizione della DG.

Ogni utente deve essere associato ad un solo profilo abilitativo in relazione al ruolo aziendale che ricopre. In caso di trasferimento o di modifica dell'attività deve essergli attribuito un profilo abilitativo corrispondente al nuovo ruolo assegnato.

l termine del rapporto di lavoro o della collaborazione le credenziali di accesso o autenticazione in uso al lavoratore verranno disattivate il giorno stesso della cessazione del rapporto o della collaborazione.

La PSW possiede una validità di 180 giorni, deve possedere almeno 8 caratteri alfanumerici e non deve contenere riferimenti agevolmente riconducibili all'utente; ogni 3 mesi l'utente deve procedere alla modifica della PSW che non potrà essere uguale alle due precedenti utilizzate. La PSW non dovrà essere annotata su documenti cartacei né digitali e non potrà essere uguale a quella utilizzata per accedere ad altri strumenti elettronici o servizi informatici dell'Ente.

Gli utenti non dovranno divulgare i propri ID e PSW né renderli noti all'interno dell'Ente, salvo per comprovate esigenze aziendali e previa autorizzazione del DG salvo non si renda necessario per la sistemazione o aggiornamento del PC o del software.

Ogni PC è dotato di misure di protezione al fine di negarne l'uso nell'ipotesi in cui l'utente, per ragioni lavorative, deve allontanarsi dalla sua postazione. Ogni PC è dotato di manualità manuale di blocco (CTRL + ALT + CANC) che l'utente dovrà azionare in caso di inutilizzo temporaneo. Ogni PC è altresì dotato di screen saver il quale entra in funzione trascorsi 10 minuti di operatività e la ripresa della sessione di lavoro richiede l'inserimento della chiave di sicurezza. In ogni caso, nessun lavoratore o collaboratore potrà lasciare incustodito o accessibile il proprio PC mentre è in corso una sessione di lavoro. Gli utenti hanno l'obbligo di spegnere il PC prima di lasciare l'ufficio.

Anche l'accesso alle Banche dati dell'Ente avviene tramite un processo di autenticazione. Ogni utente ha l'obbligo di conservare con cura l'ID e la PSW e non divulgarli.

Gli utenti che usufruiscono del servizio di posta elettronica e della rete internet per l'espletamento della propria attività lavorativa sono stati adeguatamente informati sulle modalità di utilizzo dei suddetti strumenti.

Le credenziali di accesso agli account di posta elettronica di ciascun utente corrispondono a quelle di accesso al sistema informatico. La DG può assegnare account di posta elettronica con credenziali differenti qualora lo ritenga necessario per ragioni di sicurezza. La casella di posta elettronica non può essere utilizzata per ragioni estranee al rapporto di lavoro. E' vietato l'utilizzo della casella di posta per motivi personali.

In particolare, è vietato:

- l'invio e il ricevimento di messaggi personali o la partecipazione a dibattiti, chat, aste on line, forum, concorsi;
- esprimere opinioni e commenti discriminatori;
- non divulgare notizie o informazioni riservate la cui divulgazione arrechi, anche potenzialmente, un danno all'Ente;
- ricevere, inviare o inoltrare messaggi o file la cui natura sia contraria a norme di legge;
- rispondere a e-mail di provenienza dubbia;
- utilizzare account personali e inviare messaggi file riguardanti l'attività lavorativa.

E' vietata la navigazione in internet per motivi personali. L'ente ha adottato uno specifico sistema di blocco automatico che inibisce la navigazione in determinati siti inseriti in una black list.

E' vietato l'uso dei social network per scopi personali. Solo il personale autorizzato dal proprio Responsabile dell'area di appartenenza potrà utilizzare i social network e solo ed esclusivamente per ragioni lavorative.

L'utente è responsabile di ogni azione, dichiarazione, commento, pubblicazione effettuata mediante i social

network, anche qualora l'esternazione abbia ad oggetto o riguardi, anche indirettamente, la sua attività lavorativa e/o l'Ente.

L'utente a cui viene assegnato il PC portatile ha l'obbligo di custodirlo con diligenza e dovrà periodicamente collegarsi alla rete interna dell'Ente per consentire il caricamento dell'aggiornamento del software antivirus.

Non è consentito l'uso di abbonamenti privati per collegarsi alla rete.

L'utente a cui è affidato il telefono aziendale dovrà custodirlo con diligenza; ne è vietato l'uso per scopi personali salvo diversa determinazione della DG che potrà consentirne l'uso promiscuo.

GESTIONE ARCHIVI E DOCUMENTAZIONE

Il back – up dei dati avviene tutti i giorni parziale e settimanalmente totale a cura del singolo utente operatore del PC.

La gestione dei supporti removibili del Consorzio è legata principalmente all'attività di trasferimento dei dati dall'esterno verso l'interno e trasferimento interno (tra gli apparati delle unità operative).

Se non espressamente autorizzati dalla DG, non è consentito a terzi l'utilizzo di supporti removibili sugli apparati aziendali (PC, Notebook e Server).

Ogni utente, semestralmente, provvede alla pulizia degli archivi cancellando file obsoleti o inutili.

GESTIONE FORNITORI DEI SERVIZI INFORMATICI

I Fornitori di Servizi Informatici dell'Ente dovranno condividere e sottoscrivere i principi generali di comportamento indicati nel Codice Etico e i protocolli di comportamento indicati nel presente Modello.

Ciascun contratto di consulenza e/o di fornitura di servizio e/o opere prevede clausole di riservatezza dei dati e di non divulgazione delle informazioni.

Il servizio di assistenza è garantito previa richiesta del Consorzio, vengono eseguiti specifici interventi di assistenza e manutenzione della rete aziendale.

RESPONSABILITÀ E GESTIONE DEL PROTOCOLLO

L'autorizzazione all'emissione e la diffusione del protocollo è di competenza della DG.

Ogni modifica al presente protocollo deve essere approvata dalla DG e comunicata all'Odv che valuterà l'adeguatezza e la coerenza del Modello.

DIFFUSIONE DEL PROTOCOLLO

Al fine di garantire l'efficacia del Modello, il Consorzio assicura l'ampia diffusione del protocollo e dei codici di comportamento di cui ai punti precedono, mediante consegna diretta o diffusione via e-mail.

Tale protocollo rimane, in ogni caso, a disposizione presso gli Uffici del Consorzio.