CONSORZIO DI BONIFICA
VENETO ORIENTALE
San Donà di Piave - Portogruaro

Parte speciale "L"

Reati informatici

Approvata con delibera del Consiglio di Amministrazione n. 005 del 24/01/2020

L.1 La tipologia dei reati informatici (art. 24-*bis* del Decreto)

Con l'art. 24-*bis*, si è estesa la responsabilità amministrativa dell'Ente anche in relazione ai reati informatici, di seguito descritti.

Art. 491 *bis* c.p. Documenti informatici

È un delitto contro la fede pubblica, nell'ambito della falsità di atti.

Per le falsità riguardanti un documento informatico pubblico o privato avente efficacia probatoria vanno applicate le stesse disposizioni del capo che riguardano gli atti pubblici.

Si definisce documento informatico "qualsiasi supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli".

Art. 615 *ter* c.p. Accesso abusivo ad un sistema informatico o telematico

Reato che riguarda chiunque si introduca abusivamente in un sistema informatico o telematico protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà, espressa o tacita, dell'avente diritto.

La pena è aumentata se il reo è un pubblico ufficiale o un incaricato di pubblico sevizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o un investigatore privato che esercita anche abusivamente la sua professione ovvero se vi è abuso della qualità di operatore del sistema, nonché, infine, se per commettere il reato il reo usa violenza (su persone o cose) o è palesemente armato, o se dal fatto deriva la distruzione ovvero il danneggiamento del sistema oppure di dati, informazioni e programmi in esso contenuti.

Un ulteriore aumento di pena riguarda l'abusivismo in sistemi informatici o telematici di interesse militare, o relativi all'ordine pubblico, alla sanità, o alla protezione civile o comunque di interesse pubblico.

Art. 615 *quater* c.p. Detenzione e diffusione abusive di codici di accesso a sistemi informatici o telematici

Ipotesi di reato che punisce colui che, per procurare a sé o ad altri un profitto o arrecare ad altri un danno, abusivamente si procura, riproduce, comunica, diffonde o consegna codici, parole chiave o altri mezzi che consentono l'accesso ad un sistema informatico o telematico protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo.

La pena è aumentata se ricorrono se ricorre una delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'art. 617 *quater* (vedi oltre).

Art. 615 *quinquies* c.p. Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico

Reato che condanna chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati e 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.

Art. 617 *quater* c.p. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche.

Il reato punisce chiunque fraudolentemente intercetti, impedisca o interrompa comunicazioni relative a sistemi informatici e telematici.

Salvo che il fatto costituisca più grave reato la stessa pena è comminata a coloro che rivelino il contenuto delle suddette comunicazioni, con qualsiasi mezzo di comunicazione al pubblico.

La pena è aumentata se il fatto è commesso: 1) in danno di sistemi informatici o telematici utilizzati dallo Stato, da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;

2) da pubblici ufficiali o incaricati di pubblico servizio con abuso dei poteri o 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.

Art. 617 *quinquies* c.p. Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche.

Il reato punisce chiunque installi illegalmente apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico, ovvero intercorrenti tra più sistemi.
È previsto lo stesso aggravamento di pena per le medesime ragioni del precedente art. 617 *quater* c.p. (in danno di sistemi informatici o telematici di interesse pubblico, etc.)

Art. 635 *bis* c.p. Danneggiamento di informazioni, dati e programmi informatici

Salvo che il fatto costituisca più grave reato, è punito chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui.
È previsto un aggravamento di pena qualora il fatto venga commesso con violenza o con minaccia ovvero con abuso della qualità di operatore del sistema.

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

Salvo che il fatto costituisca più grave reato, è punito 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 comunque di pubblica utilità.
La pena è aumentata qualora dal fatto derivi la distruzione, cancellazione, etc. dei dati o dei programmi informatici.
Un ulteriore aggravamento di pena è previsto se il fatto è commesso con violenza, minaccia o abuso della qualità di operatore del sistema.

Art. 635 *quater* c.p. Danneggiamento di sistemi informatici o telematici

Salvo che il fatto costituisca più grave reato, è punito chiunque mediante le condotte di cui all'art. 635 *bis* c.p., 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.
La pena è aumentata se il fatto è commesso con violenza alla persona o minaccia, oppure con abuso della qualità di operatore del sistema.

Art. 635 *quinquies* c.p. Danneggiamento di sistemi informatici o telematici di pubblica utilità

Ipotesi di reato che punisce il fatto di cui all'art. 635 *quater* c.p. diretto a distruggere, danneggiare o rendere inservibili in tutto o in parte sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.
Sono previsti degli aggravamenti di pena se dal fatto derivano la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità, ovvero se è reso inservibile, e, inoltre, se il fatto è commesso con violenza alla persona o minaccia, oppure con abuso della qualità di operatore del sistema.

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

È una particolare ipotesi di truffa che punisce (con reclusione e multa) la condotta di colui che presta servizi di certificazione di firma elettronica, il quale per procurare un ingiusto profitto a sé o ad altri, o per arrecare un danno ad altri viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

L.2 Aree a rischio

In relazione ai reati e alle condotte criminose sopra esplicitate, è da ritenersi area a rischio ogni postazione di lavoro dotata di qualsiasi terminale elettronico collegato ai sistemi informatici del Consorzio.

Vengono, altresì, considerati nel novero dei soggetti operanti in tali aree tutti coloro che, anche all'esterno delle sedi operative, utilizzano un terminale elettronico portatile con possibilità di accesso ai sistemi informatici dell'Ente.

L.3 Destinatari della parte speciale: principi generali di comportamento.

La presente Parte Speciale si riferisce a comportamenti posti in essere, oltre che dagli Amministratori, Dirigenti e Dipendenti del Consorzio, da Collaboratori Esterni e Consulenti, come già definiti nella Sezione Generale (qui di seguito, tutti definiti i "Destinatari").

Obiettivo della presente Parte Speciale è che tali soggetti si attengano a regole di condotta conformi a quanto qui prescritto, al fine di prevenire e impedire il verificarsi dei Reati Informatici.

In particolare, la presente Parte Speciale ha la funzione di:

a. fornire un elenco dei principi generali e dei principi procedurali specifici cui i Destinatari devono attenersi per una corretta applicazione del Modello;

b. fornire all'ODV e ai responsabili delle altre funzioni chiamati a cooperare con lo stesso, gli strumenti operativi necessari per le attività di controllo, monitoraggio e verifica allo stesso demandate.

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole qui contenute, i Destinatari sono tenuti a conoscere e rispettare le regole ed i principi contenuti nei seguenti documenti:

- il Codice Etico;
- il Documento Programmatico sulla Sicurezza per la gestione ed il trattamento dei dati personali ed informazioni riservate;
- il documento relativo al conferimento delle credenziali per l'accesso ai sistemi informatici del Consorzio.

L.4 Principi procedurali

Si indicano qui di seguito i principi procedurali specifici che i Destinatari sono tenuti a rispettare e che, ove opportuno, potranno essere implementati in specifiche procedure ovvero oggetto di comunicazione da parte dell'ODV.

L.4.1. Principi generali

Il Consorzio promuove l'utilizzo della rete quale strumento utile per perseguire le proprie finalità.

I Destinatari possono operare liberamente nel rispetto dei diritti degli altri utenti della rete e dei terzi, nel rispetto dell'integrità dei sistemi e delle relative risorse fisiche, in osservanza delle leggi, norme e obblighi contrattuali.

Consapevoli delle potenzialità offerte dagli strumenti informatici e telematici, i Destinatari s'impegnano ad agire con responsabilità e a non commettere abusi, aderendo ad un principio di autodisciplina.

Il posto di lavoro costituito dal terminale elettronico è consegnato completo di quanto necessario per svolgere le proprie funzioni, pertanto, è vietato modificarne la configurazione.

Il *software* installato su ciascun personal computer è quello richiesto dalle specifiche attività lavorative dell'operatore. È, pertanto, proibito installare qualsiasi programma da parte dei Destinatari o di altri operatori, escluso il referente informatico ed i suoi diretti collaboratori.

Tutti i Destinatari sono responsabili dei dati contenuti nel proprio personal computer, nonché delle modalità di memorizzazione degli stessi, secondo le indicazioni fornite.

L.4.2. Abusi e attività vietate

È proibito ogni tipo di abuso. In particolare, non è consentito, anche se ciò non dovesse integrare condotte penalmente rilevanti:

1. usare la rete in modo difforme da quanto previsto dalle leggi penali, civili e amministrative, nonché da quanto previsto dal presente Modello e dai documenti ivi richiamati;
2. utilizzare la rete per scopi incompatibili con l'attività del Consorzio;
3. utilizzare password a cui non si è autorizzati;
4. cedere a terzi codici personali (USER ID e PASSWORD) d'accesso al sistema;
5. conseguire l'accesso non autorizzato a risorse di rete interne o esterne a quella del Consorzio;
6. violare la riservatezza di altri utenti o di terzi;
7. agire deliberatamente con attività che influenzino negativamente la regolare operatività della rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti;
8. agire deliberatamente con attività che distraggano risorse (persone, capacità, elaboratori);
9. fare o permettere ad altri trasferimenti non autorizzati d'informazioni (software, archivi di dati, etc.);
10. installare o eseguire deliberatamente o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete (es: virus, cavalli di troia, worms, spamming della posta elettronica, programmi di file sharing, etc.);
11. installare o eseguire deliberatamente programmi *software* non autorizzati e non compatibili con le attività istituzionali;
12. cancellare, disinstallare, copiare, o asportare deliberatamente programmi *software* per scopi personali;
13. installare deliberatamente componenti *hardware* non compatibili con le attività istituzionali;
14. rimuovere, danneggiare deliberatamente o asportare componenti *hardware*;
15. utilizzare le risorse *hardware* e *software* e i servizi disponibili per scopi personali;

16. utilizzare le caselle di posta elettronica del Consorzio per scopi personali e/o non istituzionali;
17. utilizzare la posta elettronica con le credenziali d'accesso di altri utenti;
18. utilizzare la posta elettronica inviando e ricevendo materiale che violi le leggi;
19. utilizzare l'accesso ad Internet per scopi personali;
20. accedere direttamente ad Internet con modem collegato al proprio Personal Computer se non espressamente autorizzati e per particolari motivi tecnici;
21. connettersi ad altre reti senza autorizzazione;
22. monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività degli utenti, leggere copiare o cancellare *file* e *software* di altri utenti, senza averne l'autorizzazione esplicita dal referente informatico o suoi diretti collaboratori;
23. usare l'anonimato o servirsi di risorse che consentano di restare anonimi sulla rete;
24. inserire o cambiare le proprie password, se non dopo averla espressamente comunicata al referente informatico e essere stati espressamente autorizzati;
25. abbandonare il posto di lavoro, lasciandolo incustodito o accessibile (utilizzo di blocchi automatici a tempo).

L.4.3 Attività consentite

È consentito al referente informatico:

1. monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete e degli applicativi, per copiare o rimuovere file e software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
2. creare, modificare, rimuovere o utilizzare qualunque password, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei

dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori. il referente informatico comunicherà dell'avvenuta modifica all'utente;

3. rimuovere programmi software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
4. rimuovere componenti hardware, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.

L.4.4 Soggetti che possono avere accesso alla rete

Hanno diritto ad accedere alla rete del Consorzio i dipendenti, le ditte fornitrici di *software* per motivi di manutenzione e limitatamente alle applicazioni di loro competenza, Collaboratori Esterni impegnati nelle attività istituzionali per il periodo di collaborazione e Consulenti.

Il referente informatico può regolamentare l'accesso alla rete di determinate categorie d'utenti, quando questo è richiesto da ragioni tecniche.

Per consentire l'obiettivo di assicurare la sicurezza e il miglior funzionamento delle risorse disponibili.

Il referente informatico può proporre al titolare del trattamento l'adozione di appositi procedure di carattere operativo, che gli utenti si impegnano ad osservare.

L'accesso agli applicativi è consentito agli utenti che, per motivi di servizio, ne devono fare uso.

L.4.5. Modalità d'accesso alla rete e agli applicativi

Qualsiasi accesso alla rete e agli applicativi viene associato ad una persona fisica cui collegare le attività svolte utilizzando il codice utente.

L'utente che ottiene l'accesso alla rete e agli applicativi s'impegna ad osservare quanto stabilito dal Modello e dalle altre norme disciplinanti le attività e i servizi che si svolgono via rete e si impegna a non commettere abusi e a non violare i diritti degli altri utenti e dei terzi.
L'utente che ottiene l'accesso alla rete e agli applicativi, si assume la totale responsabilità delle attività svolte tramite la rete.
Al primo collegamento alla rete e agli applicativi, l'utente deve modificare la password secondo le indicazioni comunicategli.

L.5. Monitoraggio e segnalazione di anomalie o criticità del sistema

Ad ogni destinatario è fatto obbligo di segnalare con tempestività qualsiasi anomalia dovesse presentarsi durante l'utilizzo del proprio terminale, nonché ogni abuso dallo stesso individuato, nei tempi più solleciti possibili.
In ogni caso, i sistemi informatici adottati dal Consorzio, oltre ad essere garantiti dalle procedure indicate in premessa, genericamente riconducibili al monitoraggio costante del sistema, al blocco automatico del traffico di rete verso direttrici non standard, che garantiscono l'Ente da accessi incontrollati per qualsiasi direttrice non istituzionale, prevedono il cambio delle password e, comunque, la possibilità di variare la password in ogni momento al minimo sospetto di anomalia o criticità del sistema, nonché un sistema procedurale per la segnalazione delle non conformità.
Il referente per l'informatica o – in sua assenza – da un sostituto appositamente designato dall'Ente, con eventuale supporto tecnico da parte della ditta individuata per "servizi sistemici e di supporto", effettua inoltre periodicamente il servizio di *backup*.
La struttura informatica è coperta da diversi servizi di *backup* tra loro ridondanti.
Con cadenza mensile vengono eseguiti dei test di recupero di alcuni dati, al fine di accertare l'affidabilità del sistema.

I principali processi, nel caso di anomalia di funzionamento, inviano segnalazioni automatiche alla casella di posta elettronica di servizio *rete.informatica@bonificavenetorientale.it.*

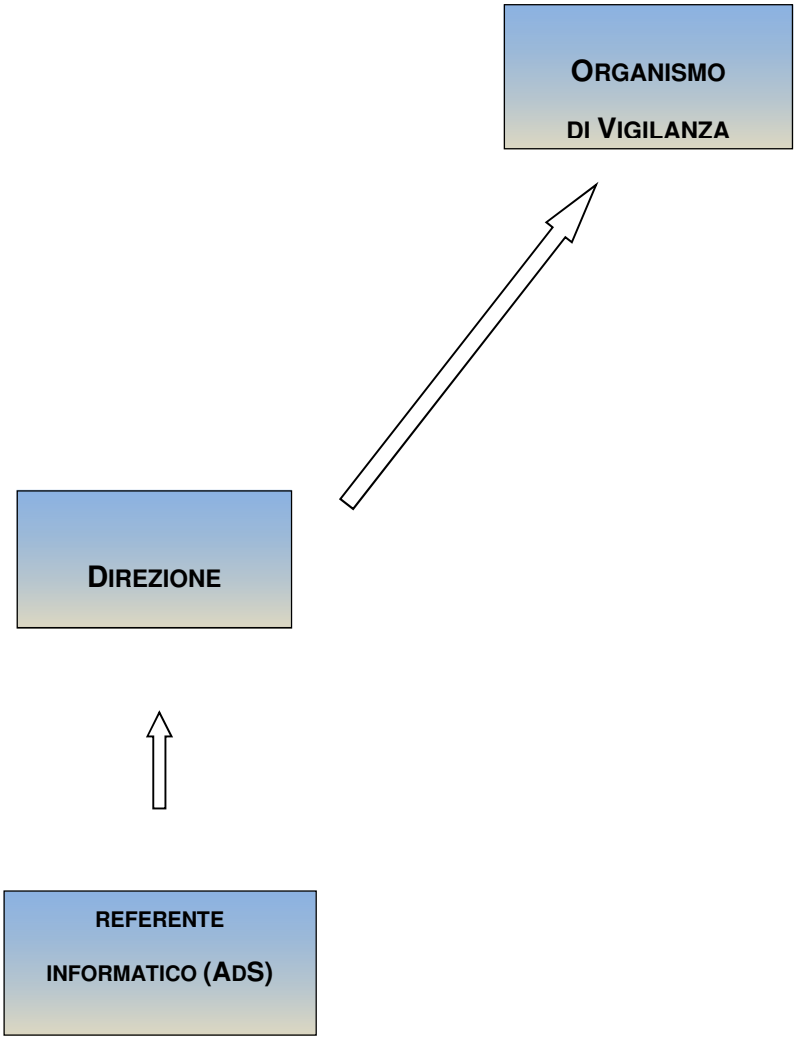
È possibile inoltre consultare la lista delle anomalie di funzionamento di ogni servizio tramite accesso alle relative *consolle* di controllo, anche da remoto.

In caso di rilevamento di anomalie o criticità del sistema, il referente informatico, cui sono affidate le operazioni di gestione dei server, nonché il mantenimento ed il buon funzionamento dei sistemi operativi, segnalerà il tutto al Direttore Generale, assumendo contemporaneamente tutte le misure provvisionali urgenti atte ad impedire il protrarsi della situazione di rischio.

Qualora infine ritenesse inquadrabile l'anomalia o le criticità nell'ambito di una potenziale condotta criminosa, riconducibile a soggetti interni o esterni al Consorzio, egli dovrà senza indugio, segnalare i fatti all'ODV, comunicando, altresì, tutti i dati necessari sulla tracciabilità delle azioni anomale e, a posteriori, individuarne la sorgente.

Il referente informatico, in relazione alle esigenze di tutela dei sistemi informatici, suggerirà al Direttore Generale, con riferimento alle rilevate anomalie, le più opportune misure e soluzioni informatiche efficaci per implementare i "sistemi di sicurezza e antri intrusione" esistenti.

TAB. 3: Schema di gestione delle informazioni in caso di anomalie



L.6. Compiti specifici dell'Organismo di Vigilanza

Anche con riferimento a quanto previsto dalla Sezione Generale del presente Modello, l'Organismo di Vigilanza è tenuto a svolgere i seguenti compiti con la massima indipendenza:

1. raccogliere, elaborare e conservare le informazioni (con particolare riferimento alle segnalazioni di cui al paragrafo precedente) rilevanti in ordine al rispetto del Modello. A tal fine, il referente informatico o Amministratore di Sistema, ha l'onere la scheda di evidenza sotto riportata, inviandola all'ODV. Parallelamente, l'ODV comunica la lista di informazioni che devono essere allo stesso ODV trasmesse;
2. condurre, in caso di segnalazione di anomalie, le indagini interne per l'accertamento di presunte violazioni delle prescrizioni in tema di utilizzo dei sistemi informatici ed eventuali condotte delittuose;
3. promuovere idonee iniziative per la diffusione della conoscenza e della comprensione degli aspetti del Modello che attengono alla politica della sicurezza informatica adottata dal Consorzio e predisporre la documentazione organizzativa interna necessaria al fine del funzionamento del Modello stesso, contenente le istruzioni, chiarimenti o aggiornamenti;
4. attivare le procedure di controllo, tenendo presente che una responsabilità primaria sul controllo delle attività, anche per quelle relative alle aree di attività a rischio, resta comunque demandata al referente informatico (amministratore di sistema);
5. segnalare al Direttore Generale le criticità e le anomalie del sistema, richiedendo i più opportuni interventi e la necessaria assistenza.

SCHEDA EVIDENZA Rischio Reati *ex* D. Lgs. n. 231/2001

Direzione / Funzione:

_____

All'Organismo di Vigilanza del Consorzio di Bonifica del Veneto Orientale

Premesso che:

- *Il Consorzio ha predisposto il proprio Modello di Organizzazione, Gestione e controllo ai sensi del D. Lgs. 231/01;*
- *tale Modello è stato approvato dal Consiglio di Amministrazione del _____/____/_____;*
- *il Modello prevede la predisposizione di Schede Evidenza delle attività svolte, da parte di ogni responsabile di Direzione/Funzione aziendale;*

nell'ambito delle proprie responsabilità operative, il sottoscritto, come previsto dal Modello Organizzativo, dichiara quanto segue:

- *Per quanto a propria conoscenza, non segnala alcuna anomalia o infrazione al Modello stesso e alle procedure aziendali in esso richiamate, ai sensi del D. Lgs. 231/2001.*
- *Sono segnalati elementi di anomalia/infrazioni in relazione alle prescrizioni del Modello:*

DESCRIZIONE DELL'EVENTO	SOGGETTI INTERNI COINVOLTI	SOGGETTI ESTERNI COINVOLTI	DATA IN CUI SI È VERIFICATO L'EVENTO

Data: ____/____/____ Firma:_____