Protocollo di comportamento n. 01

Prevenzione dei reati di cui all'art. 24 - bis del D.Lgs. 231/01

"DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI"

RIFERIMENTI NORMATIVI

Art 25-*bis* del Decreto Legislativo n. 231/2001. Artt. 491-bis, 615-ter, quater, 617-quater, quinquies, 635-bis, ter, quater, quinquies, 640-quinquies Codice Penale.

REATI IPOTIZZABILI TRA QUELLI PREVISTI DALLA NORMATIVA
Art.615 - ter C.P. - *Accesso abusivo a un sistema informatico o telematico*. Commette reato 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.
Art. 615 - quater C.P. - *Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici.* Commette reato 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 a un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo.
Articolo 615 quinquies C.P. - Diffusione di dispositivi o programmi informatici atti a danneggiare o interrompere un sistema informatico o telematico. Tale ipotesi di reato si configura nel caso in cui taluno, 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 procuri, produca, riproduca, importi, diffonda, comunichi, consegni o, comunque, metta a disposizione di altri apparecchiature, dispositivi o programmi informatici.
Art. 635 -bis C.P. - *Danneggiamento di informazioni, dati e programmi informatici* Salvo che il fatto costituisca più grave reato, commette reato chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici.
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, commette reato chiunque compie 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.

REATI IPOTIZZABILI TRA QUELLI PREVISTI DALLA NORMATIVA
Art. 635-quater C.P.- ***Danneggiamento di sistemi informatici o telematici*** Commette il presente reato chiunque, mediante le condotte dell'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.
Art. 635-quinquies C.P. - ***Danneggiamento di sistemi informatici o telematici di pubblica utilità*** Commette il presente reato chiunque, attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugga, danneggi, renda, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ne ostacoli gravemente il funzionamento.
Art. 491-bis C.P. - ***Documenti informatici.*** 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.

DESTINATARI

"Destinatari" del presente Protocollo sono tutti coloro che operano per conto della Società: il Legale Rappresentante, i dirigenti, i lavoratori, il Collegio Sindacale, nonché i collaboratori esterni che contribuiscono al conseguimento degli obiettivi della Società.

DESCRIZIONE SINTETICA DEI REATI IPOTIZZATI

La commissione di delitti informatici e di reati commessi nel trattamento illecito dei dati potrebbe avvenire durante lo svolgimento di qualsiasi attività per la quale sia richiesto l'utilizzo di una postazione informatica. In particolare il reato potrebbe configurarsi durante l'esecuzione di operazioni "on line" per la trasmissione di dati a siti istituzionali (ad esempio verso INAIL, INPS, SISTRI o altri), o durante l'accesso a portali di pubblico interesse (ad esempio: Siti dei Comuni consorziati, Siti regionali, Borsa Lavoro).

ATTIVITA' SENSIBILI E SOGGETTI COINVOLTI

Un esame delle attività svolte da HydroGEA S.p.A. ha portato all'identificazione di alcune fasi critiche che sono potenzialmente più esposte alla commissione dei reati suddetti ed all'individuazione dei soggetti coinvolti, destinatari del presente protocollo.

Nella tabella seguente sono riepilogate brevemente le attività individuate.

ESEMPI DI ATTIVITÀ ESPOSTE AL RISCHIO	SOGGETTI COINVOLTI
Accesso a portali istituzionali con password della Società per trasmissione di dati e altre operazioni on line (ad es. INAIL, INPS, Borsa Lavoro, home banking)	Legale Rappr. personale dipendente.
Nomina, formazione, attribuzione delle credenziali di accesso, controllo del personale incaricato di accedere a sistemi informatici o telematici protetti da misure di sicurezza (home banking, INAIL,…).	Legale Rappr. responsabile Sistemi Informativi, responsabile sito internet aziendale, RUP.
Installazione di programmi sui computer aziendali utilizzati dal personale dipendente in base alle funzioni ricoperte e al grado di autonomia decisionale attribuito.	Legale Rappr. responsabile Sistemi Informativi
Monitoraggio periodico delle dotazioni HW e SW.	Responsabile Sistemi Informativi
Utilizzo di posta certificata e firma elettronica (ad es. per adempimenti di legge, come per apporre data certa nel	Legale Rappr. responsabili di servizi per gli ambiti di competenza.

documento di valutazione dei rischi, comunicazioni INAIL, sistema SISTRI).	
Attività al videoterminale con accesso alla rete internet (ad es. accesso a files di sistema, programmi e altre utilità che garantiscono il funzionamento di sistemi telematici o informatici di pubblica utilità o comunque non di proprietà dell'azienda).	Tutti i dipendenti che utilizzano una postazione informatica per lo svolgimento della propria mansione.
Documentazione informatica di gestione dei rifiuti per il Sistema di controllo della tracciabilità dei rifiuti - Sistema SISTRI.	Referente generale, persone delegate all'U.L.

PRINCIPI GENERALI DI COMPORTAMENTO

La commissione Degli illeciti in argomento potrebbe avvenire durante lo svolgimento di qualsiasi attività per la quale sia richiesto l'utilizzo di una postazione informatica.

Allo scopo di vigilare sul corretto utilizzo interno delle risorse informatiche messe a disposizione, l'azienda ha pertanto nominato un **Responsabile dei Sistemi Informativi e un Responsabile del sito internet, i**ncaricandoli della gestione di tutti gli aspetti informatici aziendali e dei rapporti con l'esterno.

Il **Responsabile dei Sistemi Informativi** ha il compito di:

- registrare, in un apposito registro informatico, i software e gli hardware acquistati e installati (con i relativi numeri di licenza) e gli interventi di controllo, manutenzione e back up effettuati sugli stessi;
- verificare l'aggiornamento periodico dei software e delle password di accesso da parte dei singoli utenti;
- aggiornare periodicamente la lista dei siti vietati (black –list);
- aggiornare continuamente il sistema informatico di protezione in modo da impedire l'accesso a sistemi informatici altrui ovvero impedire la diffusione di programmi informatici che potenzialmente potrebbero danneggiare sistemi informatici altrui;
- proporre l'acquisto di hardware e di software solo da fornitori accreditati;
- proporre l'acquisti di hardware e di software che conferisce data certa ai documenti informatici solo da produttori muniti delle necessarie autorizzazioni legislative;
- in caso di problemi di entità rilevante non risolvibili internamente, rivolgersi a fornitori accreditati per richiedere un intervento manutentivo.

Il Responsabile del sito internet ha il compito di:

- vigilare sul contenuto delle informazioni pubblicate sul sito internet aziendale.

Tutti i lavoratori e i Collaboratori di HydroGEA S.p.A. sono tenuti a operare con la dovuta cura e diligenza al fine di tutelare i beni di proprietà dell'azienda, adottando comportamenti responsabili e in linea con le procedure operative predisposte per regolamentare l'utilizzo delle macchine e delle attrezzature aziendali.

In termini generali, **il personale dipendente** nell'ambito delle proprie competenze **DEVE:**

- evitare l'uso improprio di mezzi o attrezzature che gli vengono affidati, al fine di non causare costi indebiti, danni o riduzione di efficienza degli stessi e ogni altra conseguenza in contrasto con l'interesse dell'Azienda;
- evitare l'impiego dei beni di proprietà dell'azienda per scopi che esulano dalla svolgimento della attività lavorativa, inoltre evitare tassativamente di farli utilizzare o cederli a terzi salvo specifiche autorizzazioni della direzione aziendale;
- adottare e attuare in maniera scrupolosa la politica aziendale, i regolamenti e le procedure interne in modo da non compromettere la sicurezza di sistemi informatici, apparecchiature ed impianti di proprietà dell'Azienda;

- operare sempre nel rispetto delle norme di sicurezza previste dalla legge e dalle procedure interne, in modo da prevenire l'eventualità che si verifichino danni a beni, persone o all'ambiente esterno;
- segnalare tempestivamente alle funzioni preposte il verificarsi di situazioni anomale preoccupandosi, nel limite del possibile, di ridurre il rischio di furti, danneggiamenti o altre minacce ai beni ed alle risorse assegnate o presenti sul luogo di lavoro;
- segnalare eventuali anomalie e malfunzionamenti al Responsabile della comunicazione aziendale;
- trattare i dati personali necessari di persone fisiche o giuridiche necessari per lo svolgimento delle proprie mansioni con la massima discrezione, garantendo l'integrità, la disponibilità e la riservatezza dei dati stessi, nel rispetto delle normative applicabili e dei regolamenti interni;
- custodire in luogo sicuro, accessibile solo a persone debitamente autorizzate, qualsiasi hardware che conferisca data certa ai documenti informatici, prelevandolo per il tempo strettamente necessario al suo utilizzo;
- aggiornare periodicamente la propria password secondo le indicazioni aziendali.

A tutto il personale dipendente **E' VIETATO:**

- installare sul computer in dotazione qualsiasi tipo di software senza autorizzazione; di norma solo il responsabile dei sistemi informativi è autorizzato ad installare nuovi software.
- acquistare, detenere o utilizzare apparecchiature e software idonei a danneggiare programmi altrui o a danneggiare documenti informatici aventi efficacia probatoria ovvero ad alterare il software che conferisce data certa ai documenti informatici;
- conservare in luoghi facilmente accessibili copia delle password personali;
- utilizzare password di accesso o e-mail di altri utenti salvo casi di eccezionale urgenza e comunque sempre esclusivamente previa specifica autorizzazione da parte del Direttore generale;
- installare e utilizzare programmi per lo scambio di files su internet (peer-to-peer);
- installare apparecchiature hardware che potrebbero essere potenzialmente utilizzate per intercettare, impedire o interrompere comunicazioni informatiche o telematiche;
- effettuare il *download* di software gratuiti (*freeware, shareware)* che non siano strettamente attinenti all'attività lavorativa e senza la preventiva autorizzazione del Responsabile del servizio;
- effettuare transazioni finanziarie di qualsivoglia genere, comprese le operazioni di *remote banking*, acquisti on-line e simili **ad uso personale;** tali operazioni sono consentite al personale autorizzato esclusivamente per l'espletamento dell'attività lavorativa;
- registrarsi a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- partecipare a forum di carattere non professionale o non attinenti all'attività lavorativa, o utilizzare *chat line*, bacheche elettroniche o per registrarsi in *guest books* anche utilizzando pseudonimi, senza la preventiva autorizzazione della Direzione;
- navigare su internet e accedere a caselle web-mail di posta elettronica personale durante l'orario di lavoro. La navigazione per scopi personali e l'accesso alle caselle di posta privata sono consentiti **esclusivamente** nelle ore extralavorative; in ogni caso **E' ASSOLUTAMENTE VIETATO** navigare o registrarsi in siti il cui contenuto risulti discriminatorio, sessuale, pedo-pornografico, offensivo, discutibile o, comunque, inopportuno e contro i principi enunciati nel Codice Etico aziendale.

DOCUMENTAZIONE AZIENDALE DI RIFERIMENTO

- Statuto sociale
- Codice etico
- Modello di organizzazione e di gestione ai sensi del D.Lgs. 231/01
- Comunicazioni interne e ordini di servizio
- Regolamenti, Procedure, istruzioni e moduli interni.

ALTRI RIFERIMENTI DOCUMENTALI

- Contratti in essere con ditte esterne per la manutenzione dell'hardware e del software di proprietà dell'azienda.

SISTEMA DI CONTROLLO "231"

L'OdV, secondo quanto stabilito dal proprio Regolamento, può effettuare i controlli previsti in qualsiasi momento, richiedendo tutta la documentazione del caso.

I destinatari del presente protocollo dovranno pertanto mettersi a disposizione dell'OdV rispondendo prontamente a tutte le richieste che verranno avanzate, come ad esempio la predisposizione e l'emanazione di procedure standardizzate relative ai comportamenti da seguire nell'ambito delle aree di rischio.

In particolare, l'OdV provvede all'espletamento dei propri compiti:

- svolgendo verifiche documentali, sia periodiche che a campione;
- valutando l'efficacia delle procedure in essere e, se del caso, richiedendone di nuove;
- esaminando eventuali segnalazioni.

FLUSSI INFORMATIVI VERSO L'OdV

Chiunque può rivolgersi all'OdV in qualsiasi momento, nei modi previsti dal Regolamento dell'Organismo di Vigilanza, sia per segnalare fatti e/o notizie rilevanti ai fini della prevenzione dei reati previsti del Decreto sia per suggerire proposte e interventi.

Al fine di espletare le proprie funzioni di controllo, in aggiunta ai flussi "spontanei" di cui sopra, l'OdV può richiedere la trasmissione periodica di precise informazioni o documenti, previa definizione della periodicità, dei contenuti dell'invio e dei soggetti incaricati.