

COIMA SGR S.p.A. –

Società di Gestione del Risparmio

**MODELLO DI ORGANIZZAZIONE E GESTIONE
AI SENSI DEL DECRETO LEGISLATIVO
8 GIUGNO 2001, N. 231**

**PARTE SPECIALE “G”
REATI INFORMATICI E DI TRATTAMENTO ILLECITO DI DATI**

	MODELLO DI ORGANIZZAZIONE E GESTIONE	Revisione 12 Pagina 2 di 9
---	---	--

PARTE SPECIALE “G” – REATI INFORMATICI E DI TRATTAMENTO ILLECITO DI DATI

1. Le “attività sensibili” ai fini del D.lgs. n. 231/2001

L’art. 6, comma 2, lett. a) del D.lgs. n. 231/2001 indica, come uno degli elementi essenziali dei modelli di organizzazione e di gestione previsti dal decreto, l’individuazione delle cosiddette attività “sensibili” o “a rischio”, ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal D.lgs. n. 231/2001.

Il nucleo delle ipotesi di reato, oggetto della presente Parte Speciale, con riferimento specifico a COIMA SGR S.p.A. (“COIMA SGR”), si rinviene in attività consistenti nell’accesso abusivo ad un sistema; in dettaglio, l’ipotesi di accesso abusivo ricorre:

- sia nei casi in cui abbia ad oggetto un sistema che è interconnesso a una rete (ad es, internet) per cui non si possiede alcun tipo di autorizzazione, nella quale ipotesi l’autore del reato effettua connessioni triangolate su server esteri in modo da complicare la ricostruzione del percorso d’accesso;
- sia quando lo si effettui ai danni di un sistema rispetto al quale si dispone di credenziali, ma per una funzione differente da quella per cui avviene l’accesso. Tale condotta appare facilmente integrabile in relazione a una rete aziendale, ove i dipendenti accedano a un’area del server aziendale, senza esservi autorizzati. Il caso potrebbe verificarsi ove il dipendente sottraesse le credenziali di un collega onde accedere ad ambiti allo stesso vietati.

L’accesso abusivo è punito a prescindere dalla finalità per cui venga posto in essere e dal danneggiamento dello stesso: tuttavia, premesso che nella generalità dei casi i sistemi informatici o telematici sono protetti da misure di sicurezza, appare assai improbabile che l’accesso prescinda da rimozioni di sicurezze, alterazione di password o altre forzature del sistema, tali da integrare forme di danneggiamento.

L’analisi dei processi aziendali di COIMA SGR ha consentito di individuare le attività nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate dall’art. 24-*bis* del D.lgs. n. 231/2001. Qui di seguito sono elencati i processi esaminati unitamente alle attività sensibili identificate al loro interno e le funzioni/unità organizzative coinvolte di COIMA SGR:

1) **Gestione dei sistemi informativi e della sicurezza informatica:** trattasi delle attività inerenti i sistemi propri di COIMA SGR ed, in particolare, le attività di gestione del sito internet e della rete intranet, gestione dei profili utente e del processo di autenticazione, gestione dell'hardware e del software aziendale, gestione del processo di creazione, trattamento, archiviazione di documenti elettronici con valore probatorio, protezione della postazione di lavoro, gestione degli accessi da e verso l'esterno, gestione e protezione delle reti informatiche, delle banche dati e degli output di sistema e dei dispositivi di memorizzazione nonché la sicurezza fisica (cablaggi, dispositivi di rete, ecc.).

➤ **Principali Funzioni/Unità Organizzative coinvolte:**

Amministratore Delegato, Finance, Human Resources, Organization, Information & Digital Transformation.

➤ **Reati ipotizzabili:**

- Accesso abusivo a sistema informatico (art. 615-ter c.p.)
- Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)
- Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.)
- Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-quater c.p.)

2) **Gestione dei flussi informativi mediante accesso a Sistemi Informativi di terzi:** si tratta delle attività di trasmissione, caricamento, anche mediante accesso a sistemi informatici di terzi, di dati, informazioni, attinenti la gestione di COIMA SGR (ad esempio Accesso a Infostat di Banca d'Italia, Accesso ai sistemi di Tele-raccolta di Consob).

➤ **Principali Funzioni/Unità Organizzative coinvolte:**

Amministratore Delegato, Finance, Information & Digital Transformation, Organization.

➤ **Reati ipotizzabili:**

- Accesso abusivo a sistema informatico (art. 615-ter c.p.)
- Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-quater 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.)

	MODELLO DI ORGANIZZAZIONE E GESTIONE	Revisione 12 Pagina 4 di 9
---	---	--

- 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.)

2. Il sistema dei controlli

Il sistema dei controlli, perfezionato da COIMA SGR sulla base delle indicazioni fornite dalle principali associazioni di categoria, quali le Linee guida Confindustria, prevede con riferimento alle attività sensibili e ai processi strumentali individuati:

- principi generali di comportamento relativi alle attività sensibili;
- protocolli di controllo “specifici” applicati alle singole attività sensibili.

I protocolli di controllo sono fondati sulle seguenti regole generali, che devono essere rispettate nell’ambito di ogni attività sensibile individuata:

- **Segregazione dei compiti:** preventiva ed equilibrata distribuzione delle responsabilità e previsione di adeguati livelli autorizzativi, idonei ad evitare commistione di ruoli potenzialmente incompatibili o eccessive concentrazioni di responsabilità e poteri in capo a singoli soggetti. In particolare deve essere garantita la separazione delle attività e responsabilità tra chi autorizza, chi esegue e chi controlla una determinata operazione nelle attività sensibili.
- **Norme:** esistenza di disposizioni aziendali e/o di procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante.
- **Poteri autorizzativi e di firma:** i poteri autorizzativi e di firma devono essere:
 - i) coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, indicazione delle soglie di approvazione delle spese;
 - ii) chiaramente definiti e conosciuti all’interno di COIMA SGR.
- **Tracciabilità:**
 - (i) ogni operazione relativa all’attività sensibile deve essere, ove possibile, adeguatamente registrata;
 - (ii) il processo di decisione, autorizzazione e svolgimento dell’attività sensibile deve essere verificabile *ex post*, anche tramite appositi supporti documentali;
 - (iii) in ogni caso, deve essere disciplinata in dettaglio la possibilità di cancellare o distruggere le registrazioni effettuate.

2.1 Principi generali di comportamento prescritti nelle attività sensibili

Divieti

	MODELLO DI ORGANIZZAZIONE E GESTIONE	Revisione 12 Pagina 5 di 9
---	---	--

La presente Parte Speciale prevede l'espresso divieto - a carico degli Esponenti Aziendali, in via diretta, ed a carico dei Collaboratori esterni e Partner, tramite apposite clausole contrattuali - di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato sopra considerate (art. 24-*bis* del D.lgs. 231/2001);
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo.

In particolare è fatto divieto di:

- alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
- accedere abusivamente al sistema informatico o telematico di COIMA SGR e di altri soggetti terzi, con cui COIMA SGR intrattiene rapporti nell'ambito della propria attività, al fine di alterare e /o cancellare dati e/o informazioni;
- detenere e/o utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico di COIMA SGR e degli altri soggetti terzi, con cui COIMA SGR intrattiene rapporti nell'ambito della propria attività, al fine di acquisire informazioni riservate;
- svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di COIMA SGR e degli altri soggetti terzi, con cui COIMA SGR intrattiene rapporti nell'ambito della propria attività, al fine di acquisire informazioni riservate;
- svolgere abusivamente attività di modifica e/o cancellazione di dati, informazioni o programmi di COIMA SGR e degli altri soggetti terzi, con cui COIMA SGR intrattiene rapporti nell'ambito della propria attività;
- svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
- distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità;
- trasferire all'esterno di COIMA SGR e/o trasmettere file, documenti, o qualsiasi altra documentazione riservata di proprietà di COIMA SGR, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione dell'Amministratore Delegato;
- lasciare accessibile ad altri il proprio PC oppure consentire l'utilizzo dello stesso ad altre persone (parenti, amici, ecc.);
- utilizzare abusivamente password di altri utenti aziendali, neppure per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione del responsabile di funzione;

	MODELLO DI ORGANIZZAZIONE E GESTIONE	Revisione 12 Pagina 6 di 9
---	---	--

- utilizzare strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici.

Doveri

La presente sezione prevede l'espresso obbligo a carico dei soggetti sopra indicati di conoscere e rispettare:

- tutte le misure atte a garantire l'affidabilità del sistema tenendo conto anche dell'evoluzione tecnologica, per quanto riguarda: la sicurezza dei dati trattati, il rischio di distruzione o di perdita ed il rischio di accesso non autorizzato o non consentito.

È inoltre tassativamente imposto di:

- rispettare le procedure denominate "Piano di continuità operativa", "Procedura gestione degli incidenti di sicurezza informativa", "Procedura Identity and Access management", "Procedura Operazioni IT", "Procedura ICT risk management", "Policy IT", "Modello organizzativo Privacy";
- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure di COIMA SGR interne, in tutte le attività finalizzate alla fornitura di servizi a favore dei propri iscritti;
- assicurare un pieno rispetto delle norme di legge e regolamenti, nonché delle procedure di COIMA SGR interne, nell'acquisizione, elaborazione e comunicazione dei dati e delle informazioni, sia ai fini interni che nello svolgimento delle attività istituzionali a favore dei propri iscritti;
- effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti di Consob, Borsa Italiana non frapponendo alcun ostacolo all'esercizio delle funzioni di vigilanza da queste esercitate;
- predisporre efficaci piani di sicurezza e sistematici monitoraggi della rete interna (intranet) di COIMA SGR al fine di evitare la commissione di reati.

2.2 Standard di controllo specifici

Qui di seguito sono elencati i protocolli di controllo specifici relativi alle singole attività sensibili individuate:

1) Gestione dei sistemi informativi e della sicurezza informatica

Con riferimento a tale area sensibile è necessario seguire tali protocolli:

- definire con chiarezza ruoli e compiti delle Funzioni responsabili della gestione delle varie fasi del processo sensibile ed, in particolare, (i) della gestione delle modalità di accesso di utenti interni a COIMA SGR e gli obblighi dei medesimi nell'utilizzo dei

sistemi informatici; (ii) della gestione delle modalità di accesso di utenti esterni a COIMA SGR e gli obblighi dei medesimi nell'utilizzo dei sistemi informatici, (iii) della gestione dei rapporti con i terzi in caso di accesso, gestione, comunicazione, fornitura di prodotti/servizi per l'elaborazione dei dati e informazioni da parte degli stessi terzi;

- prevedere controlli al fine di prevenire accessi non autorizzati, danni e interferenze ai locali e ai beni in essi contenuti tramite la messa in sicurezza delle aree e delle apparecchiature;
- assicurare la correttezza e la sicurezza dell'operatività dei sistemi informativi tramite *policy* e procedure. In particolare si rende necessario garantire: (i) il corretto e sicuro funzionamento degli elaboratori di informazioni; (ii) la protezione da software pericoloso; (iii) il backup di informazioni e software; (iv) la protezione dello scambio di informazioni attraverso l'uso di tutti i tipi di strumenti per la comunicazione anche con terzi; (v) una verifica dei log che registrano le attività degli utilizzatori, le eccezioni e gli eventi concernenti la sicurezza; (vi) il controllo sui cambiamenti agli elaboratori e ai sistemi; (vii) la gestione di dispositivi rimovibili;
- monitorare gli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi, alle applicazioni. In particolare si rende necessario prevedere mediante *policy* interna: (i) l'autenticazione individuale degli utenti tramite codice identificativo dell'utente e password o altro sistema di autenticazione sicura; (ii) liste di controllo del personale abilitato all'accesso ai sistemi, nonché le autorizzazioni specifiche dei diversi utenti o categorie di utenti; (iii) una procedura di registrazione e deregistrazione per accordare e revocare l'accesso a tutti i sistemi e servizi informativi; (iv) la rivisitazione dei diritti d'accesso degli utenti secondo intervalli di tempo prestabiliti usando un processo formale; (v) l'accesso ai servizi di rete esclusivamente da parte degli utenti che sono stati specificatamente autorizzati e le restrizioni della capacità degli utenti di connettersi alla rete; (vi) la custodia dei dispositivi di memorizzazione (ad es. chiavi USB, CD, hard disk esterni, etc.) e l'adozione di regole di *clear screen* per gli elaboratori utilizzati;
- definire adeguate modalità per il trattamento degli incidenti e dei problemi relativi alla sicurezza informatica;
- prevedere attività di verifica periodica dell'efficienza ed efficacia della gestione della sicurezza informatica;
- le persone destinate a svolgere attività IT (ivi incluso l'amministratore di sistema) devono essere scelte con criteri trasparenti, previa valutazione dell'esperienza maturata con particolare riferimento alla sicurezza dei sistemi informativi;
- organizzare specifiche attività di formazione e aggiornamenti periodici sulle procedure aziendali di sicurezza informatica per tutti i dipendenti e, dove rilevante, per i terzi.

Inoltre devono essere osservati i seguenti ulteriori obblighi:

- attenersi alle istruzioni impartite secondo il Regolamento Europeo GDPR in tema di trattamento dei dati personali;
- rispettare quanto previsto dal documento denominato “Disciplinare interno per l'utilizzo della posta elettronica ed internet”;
- utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente nell'ambito dell'attività svolta da COIMA SGR;
- non prestare o cedere a terzi qualsiasi apparecchiatura informatica, senza la preventiva autorizzazione del responsabile della funzione competente alla gestione dei relativi sistemi informatici;
- in caso di smarrimento o furto di qualsiasi apparecchiatura informatica della Società, informare tempestivamente l'Amministratore Delegato e presentare denuncia all'autorità giudiziaria;
- utilizzare la connessione internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che rendono necessario il collegamento;
- astenersi dall'effettuare copie non specificamente autorizzate di dati e di software.

A tal fine è necessario il rispetto della procedura “Procedura di gestione delle risorse umane”, insieme alle procedure inerenti la gestione informatica espressamente richiamate al paragrafo 2.1.

2) Gestione dei flussi informativi mediante accesso a Sistemi Informativi di terzi

Con riferimento a tale area sensibile è necessario seguire tali protocolli:

- prevedere una chiara segregazione dei ruoli e dei compiti delle Funzioni responsabili della gestione delle varie fasi del processo sensibile; ed, in particolare, (i) della gestione delle modalità di accesso di COIMA SGR ai sistemi informatici e telematici di soggetti terzi, con cui COIMA SGR intrattiene rapporti nell'ambito della propria attività; (ii) della gestione dei rapporti con i soggetti terzi, con cui COIMA SGR intrattiene rapporti nell'ambito della propria attività ai fini dell'accesso, gestione, comunicazione dei dati per l'elaborazione delle informazioni destinate al mercato;
- prevedere controlli al fine di prevenire accessi non autorizzati, danni e interferenze presso COIMA SGR ed i soggetti terzi, con cui COIMA SGR intrattiene rapporti nell'ambito della propria attività;
- prevedere regole chiare e precise al fine di prevenire la detenzione e/o l'utilizzo abusivo di codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico dei soggetti terzi, con cui COIMA SGR intrattiene rapporti nell'ambito della propria attività;
- monitorare gli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi, alle applicazioni presso i soggetti terzi, con cui COIMA SGR intrattiene rapporti nell'ambito della propria attività;

	MODELLO DI ORGANIZZAZIONE E GESTIONE	Revisione 12 Pagina 9 di 9
---	---	--

- definire adeguate modalità per il trattamento degli incidenti e dei problemi relativi alla sicurezza informatica.

A tal fine è necessario il rispetto della procedura denominata “Procedura di gestione delle risorse umane”, insieme alle procedure inerenti la gestione informatica espressamente richiamate al paragrafo 2.1.