Modello di organizzazione, gestione e controllo ai sensi del Decreto Legislativo 8 Giugno 2001, n. 231

Protocollo 09
Gestione dei sistemi informativi

Approvato dal Consiglio di Amministrazione con delibera del 03 agosto 2022

Indice

Definizioni

- **Attività Sensibili**: attività della Società nel cui ambito sussiste il rischio di commissione di reati di cui al Decreto o rilevanti per la gestione delle risorse finanziarie.
- **Codice Etico**: Codice Etico adottato dalla Società**.**
- **D.Lgs. 231/2001 o Decreto**: Decreto Legislativo 8 giugno 2001, n. 231.
- **LCM o Società**: Latteria e Caseificio Moro S.r.l.
- **Modello 231 o Modello**: modello organizzativo adottato dalla Società ai sensi del D.Lgs. 231/2001.
- **Organismo di Vigilanza o OdV**: l'organismo, interno all'ente, dotato di autonomi poteri di iniziativa e di controllo, che, ai sensi dell'art. 6 del Decreto, ha il compito di vigilare sul funzionamento e l'osservanza del modello di organizzazione, gestione e controllo e di curarne l'aggiornamento.

Scopo

Il presente protocollo ha lo scopo di presidiare le aree di attività aziendali a rischio-reato nell'ambito della gestione dei sistemi informativi condotte dai destinatari del Modello come identificati dalla Parte Generale del Modello stesso.
Coerentemente con la Parte Generale del Modello, il documento definisce le linee guida comportamentali nonché i presidi operativi di controllo a cui tutti i destinatari si attengono nello svolgimento della propria attività al fine di prevenire o mitigare il rischio di commissione dei reati presupposto di cui agli artt. 24-*bis*, 25-*novies* e 25-*quinquiesdecies* D.Lgs. 231/2001.
Il presente protocollo, redatto in conformità alle previsioni del D.Lgs. 231/2001, costituisce pertanto parte integrante del Modello.

Destinatari e ambito di applicazione

Il presente protocollo si applica ai responsabili delle Funzioni, ai loro diretti riporti gerarchici, nonché a qualsiasi altro destinatario del Modello che risulti a vario titolo coinvolto nell'Attività Sensibile:

- *Gestione dei sistemi informativi*.

Riferimenti

- D.Lgs. 231/2001 "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica*";
- Modello organizzativo ai sensi del D.Lgs. 231/2001 – Parte Generale;

- Codice Etico;
- Documentazione a supporto delle Attività Sensibili.

Principi generali di comportamento

I destinatari a qualsiasi titolo coinvolti nella gestione dei sistemi informativi in ordine agli ambiti di applicazione sopra richiamati sono tenuti a osservare, oltre alle previsioni del presente protocollo, le norme di legge applicabili, i principi di condotta previsti nel Codice Etico nonché i principi previsti nella Parte Generale del Modello.

È fatto **divieto** di:

- introdursi abusivamente in un sistema informatico o telematico protetto da misure di sicurezza;
- accedere a un sistema informatico o telematico non possedendo le credenziali d'accesso o utilizzando le credenziali di altri colleghi abilitati;
- detenere, procurarsi o diffondere abusivamente codici di accesso o comunque mezzi idonei all'accesso di un sistema protetto da misure di sicurezza;
- utilizzare dispositivi tecnici o *software* non autorizzati e/o atti a impedire o interrompere le comunicazioni relative a un sistema informatico o telematico;
- distruggere, danneggiare, cancellare, alterare informazioni, dati o programmi informatici altrui e di pubblica utilità;
- utilizzare *software* non fornito sul proprio supporto originale o comunque dal soggetto detentore dei diritti d'autore relativi allo stesso, nonché in numero superiore alle licenze acquistate dalla Società;
- riprodurre, diffondere o comunque mettere a disposizione di altri *software* senza il consenso del soggetto detentore dei diritti d'autore relativi allo stesso;
- lasciare incustodito e/o accessibile ad altri il PC assegnato dalla Società.

È fatto **obbligo** di:

- informare tempestivamente il responsabile dell'ufficio di appartenenza in caso di smarrimento o furto delle attrezzature informatiche aziendali;
- attenersi alle *policy* adottate dalla Società che disciplinano l'utilizzo dei sistemi e degli applicativi informatici della Società stessa.

Presidi di controllo specifici per Attività Sensibile

1. Gestione dei sistemi informativi

Con riferimento all'Attività Sensibile in oggetto:

- la separazione dei compiti è garantita dal coinvolgimento dei diversi responsabili di funzione secondo la relativa competenza.
  La Società si avvale del supporto di diversi consulenti a seconda dei servizi (ad es. *software*, sito *web* e posta elettronica, risoluzione problemi di rete);
- l'Attività Sensibile in esame è regolata da una specifica procedura/*policy* che disciplina le fasi principali, gli attori coinvolti, i relativi ambiti di intervento e di responsabilità, le modalità di tracciabilità e documentabilità, con particolare riferimento a:
  - gestione degli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi, alle applicazioni;
  - gestione della sicurezza fisica;
  - gestione degli incidenti e dei problemi di sicurezza informatica;
  - gestione e protezione delle reti;
  - gestione della sicurezza fisica dei centri di elaborazione dati e locali tecnici IT;
  - gestione del processo di assegnazione e dismissione degli asset IT, siano essi *software* (ad es. licenze) o *hardware*;
  - gestione del processo di classificazione e controllo dei beni (sia *hardware* sia *software*);
  - gestione delle comunicazioni e dell'operatività (scambio di informazioni, *log management*, *patch management*, politiche di *backup*, ecc.);
  - misure di sicurezza dell'operatività e delle comunicazioni;
  - gestione del processo di acquisizione, sviluppo e manutenzione di apparecchiature, dispositivi o programmi informatici;
  - archiviazione della documentazione.
- la tracciabilità e la verificabilità *ex post* delle attività riconducibili all'Attività Sensibile in esame sono garantite dall'archiviazione della documentazione prodotta durante le varie fasi della stessa a cura delle Funzioni coinvolte, in linea con le modalità di archiviazione previste dalla citata procedura.

I FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA 231

Al fine di rendere effettivo l'esercizio delle sue funzioni, l'Organismo di Vigilanza deve poter essere informato in merito a fatti od eventi che potrebbero ingenerare responsabilità della Società ai sensi del D.Lgs. n. 231/2001. È necessario che sia definito ed attuato un costante scambio di informazioni tra i destinatari del Modello 231 e l'Organismo di Vigilanza stesso.

In particolare, nel Modello 231 adottato vengono individuate due tipologie di flussi informativi diretti all'Organismo di Vigilanza:

1. Segnalazioni
2. Flussi informativi periodici

1. SEGNALAZIONI: da inviare in caso di rilevazione di gravi comportamenti illegali (frode, corruzione, etc.) o più in generale di comportamenti non corretti nella conduzione del lavoro e degli affari in violazione del Modello 231.
   Tutti soggetti coinvolti nelle attività sensibili sono, infatti, tenuti a segnalare tempestivamente all'Organismo di Vigilanza, tramite i canali informativi specificamente identificati:
   • violazioni di leggi e norme applicabili;
   • violazioni, conclamate o sospette, del Modello o delle procedure ad esso correlate o degli elementi che lo compongono;
   • comportamenti e/o pratiche non in linea con le disposizioni del Codice Etico adottato dalla società;
   • eventuali deroghe alle procedure decise in caso di emergenza o di impossibilità temporanea di attuazione, indicando la motivazione ed ogni anomalia significativa riscontrata.

   La società si è dotata di un'apposita piattaforma "Whistleblowing" fornita di ISWeb Spa, accessibile da parte di tutti gli interessati, finalizzata a procedere alle segnalazioni in forma anonima. La società si è dotata altresì di un'apposita casella di posta elettronica odv231@caseificiomoro.com accessibile da parte di tutti gli interessati, finalizzata a procedere alle segnalazioni firmate.

2. FLUSSI INFORMATIVI PERIODICI: si tratta di informazioni e notizie provenienti dalle singole Funzioni aziendali coinvolte nelle attività a rischio, sia di propria iniziativa che su richiesta dell'Organismo di Vigilanza, relative a fattispecie rilevanti e ad eventuali criticità individuate nell'ambito dell'area aziendale di appartenenza, al fine di consentire all'Organismo stesso di monitorare l'insorgenza di attività sensibili, il funzionamento e l'osservanza del Modello.

Archiviazione

Tutta la documentazione prodotta nell'ambito delle attività disciplinate nel presente protocollo, comprese eventuali comunicazioni a mezzo posta elettronica, è conservata a cura della Funzione di volta in volta coinvolta e messa a disposizione, su richiesta, del Consiglio di Amministrazione, del Collegio Sindacale e dell'Organismo di Vigilanza.

I documenti prodotti nell’ambito delle attività descritte nel presente protocollo devono essere conservati per un periodo di almeno cinque anni, salvo diverse previsioni legislative.