INTEGRA LIFESCIENCES ITALY S.R.L.

Modello di Organizzazione, Gestione e Controllo

(adottato ai sensi del Decreto Legislativo n. 231/2001)

Parte speciale J

Gestione dei Sistemi Informativi

1. Finalità

La presente Parte Speciale ha la finalità di definire i principi di comportamento ed i presidi di controllo che i Destinatari coinvolti nella gestione delle attività / processi elencati al successivo par. 2 devono osservare al fine di prevenire il rischio di commissione dei reati previsti dal D.Lgs. 231/2001 e di assicurare condizioni di correttezza e trasparenza nella conduzione delle attività aziendali.

Nello specifico, la presente Parte Speciale ha lo scopo di:

- indicare i principi di comportamento ed i presidi di controllo che i Destinatari devono osservare ai fini della corretta applicazione del Modello;
- fornire all'Organismo di Vigilanza e alle altre strutture di controllo gli strumenti per esercitare le attività di monitoraggio, controllo, verifica.

In linea generale, tutti i Destinatari dovranno adottare, ciascuno per gli aspetti di propria competenza, comportamenti conformi al contenuto dei seguenti documenti:

- Parte Generale del Modello;
- Standard of Business Conduct and Ethics;
- sistema di procure e deleghe in vigore;
- ogni altro documento aziendale che regoli attività rientranti nell'ambito di applicazione del Decreto.

È inoltre espressamente vietato adottare comportamenti contrari a quanto previsto dalle vigenti norme di legge.

2. Ambito di applicazione e aree sensibili

La presente Parte Speciale e, nello specifico, i principi di comportamento e di controllo descritti ai paragrafi seguenti, si applicano a tutti gli esponenti aziendali e, in particolare, a coloro che, in ragione del proprio incarico o della propria funzione, si trovino a operare nell'ambito dei processi di "Gestione dei Sistemi Informativi".

3. Reati potenzialmente rilevanti

I reati che la Società ritiene potenzialmente applicabili nell'ambito della conduzione delle attività in oggetto (si rimanda all'Allegato 1 del Modello *"Catalogo dei reati e illeciti amministrativi presupposto del D.Lgs. 231/2001"* per una descrizione di dettaglio di ciascuna fattispecie di reato richiamata) sono:

- delitti informatici e trattamento illecito dei dati (art. 24 D.Lgs. 231/2001) e in particolare:
  - art. 491-bis c.p. - Documenti informatici;
  - art. 615-ter c.p. - Accesso abusivo ad un sistema informatico o telematico;
  - art. 615-quater c.p. - Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici;

  - art. 617-quater c.p. - Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche;
  - art. 617-quinquies c.p. - Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche;
  - art. 635-bis c.p. - Danneggiamento di informazioni, dati e programmi informatici;
  - art. 635-quater c.p. - Danneggiamento di sistemi informatici o telematici;
- delitti in materia di violazione del diritto d'autore (art. 25-novies D.Lgs. 231/2001) e in particolare:
  - art. 171-bis L. 633/41 co. 1- Abusiva duplicazione, per trarne profitto, di programmi per elaboratore;
- reati tributari (art. 25-quinquiesdecies del D.Lgs. 231/2001), in particolare:
  - art. 10 D.Lgs. 74/2000 - Occultamento o distruzione di documenti contabili.

4. Principi di comportamento

Gli esponenti aziendali che, in ragione del proprio incarico o della propria funzione, siano coinvolti nell'ambito delle attività in oggetto, devono:

- attenersi rigorosamente alle procedure aziendali in materia di gestione degli asset aziendali e, in particolare, della rete informatica di Integra, in ogni caso facendone un uso appropriato rispetto alle proprie mansioni lavorative;
- astenersi da qualsiasi condotta che possa compromettere la sicurezza, riservatezza e integrità delle informazioni e dei dati aziendali e dei terzi;
- astenersi da qualsiasi condotta diretta a superare o aggirare le protezioni del sistema informatico aziendale della Società o altrui (si tratti di soggetti pubblici o di soggetti privati);
- attenersi all'utilizzo univoco e individuale dei codici identificativi (user-id) per l'accesso alle applicazioni e alla rete;
- attenersi a una corretta gestione delle password attraverso l'osservanza delle linee guida, comunicate a tutti gli utenti per la selezione e l'utilizzo della parola chiave;
- verificare periodicamente gli accessi effettuati dagli utenti, in qualsiasi modalità, ai dati, ai sistemi e alla rete;
- garantire la tracciabilità, attraverso le applicazioni, delle modifiche ai dati compiute dagli utenti;
- definire i criteri e le modalità per l'assegnazione, la modifica e la cancellazione dei profili utente;
- analizzare periodicamente i profili utente al fine di verificare che siano coerenti con le responsabilità assegnate;
- definire le misure di sicurezza adottate, le modalità di vigilanza e la relativa frequenza, la responsabilità, il processo di reporting delle violazioni / effrazioni dei locali tecnici o delle misure di sicurezza, le contromisure da attivare;

- archiviare la documentazione riguardante ogni singola attività allo scopo di garantire la completa tracciabilità della stessa.

È inoltre espressamente vietato:

- accedere abusivamente (senza previa autorizzazione) ad un sistema informatico protetto;
- alterare, mediante l'utilizzo di firma elettronica altrui o comunque in qualsiasi modo, documenti informatici nonché dati ed informazioni contenute nei programmi informatici;
- distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui o anche solo mettere in pericolo l'integrità e la disponibilità di informazioni, dati o programmi utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti o comunque di pubblica utilità;
- produrre e trasmettere documenti in formato elettronico con dati falsi e/o alterati;
- ottenere, riprodurre, diffondere, comunicare o divulgare codici di accesso a sistemi informatici protetti o criptati;
- installare apparecchiature atte ad intercettare terze parti e carpire informazioni che possono essere di interesse o vantaggio per la Società;
- installare apparecchiature atte al danneggiamento dei sistemi hardware che abbia il fine di procurare un interesse o vantaggio per la Società (ad es. accesso alle copie di backup e distruzione di informazioni che possano essere prova di azioni illecite);
- diffondere programmi capaci di infettare un sistema per manometterne la regolare funzionalità (ad es. il sistema informatico di un competitor);
- utilizzare illecitamente un software protetto da diritto d'autore senza aver acquistato, in tutto o in parte, le dovute licenze;
- duplicare abusivamente programmi coperti da licenza al fine di trarne vantaggi in termini di risparmio di costi;
- inserire nel sito web aziendale opere dell'ingegno protette dal diritto d'autore, ovvero parti di esse, di cui l'azienda non abbia acquisito regolare licenza (si pensi, ad esempio, a pubblicazioni scientifiche relative a farmaci o emoderivati commercializzati dalle aziende del Gruppo);
- occultare o distruggere le scritture contabili o altri documenti assimilati memorizzati e archiviati sui sistemi informativi utilizzati dalla Società, al fine di non rendere ricostruibile il reddito o il volume d'affari.

5. Gestione dei Sistemi Informativi

Le attività inerenti alla gestione dei sistemi informativi (i.e.: Global Technology / Information System) sono in capo alla Funzione di Information Technology di Corporate in forza di uno specifico contratto di service, a cui si rimanda.

Si elencano di seguito i presidi di controllo che devono essere posti in essere nell'ambito della gestione dei Sistemi Informativi.

Gestione degli accessi logici ai dati e ai sistemi

- Ogni dipendente è fornito di un'utenza logica e ha a disposizione un PC connesso alla rete aziendale;
- l'accesso agli applicativi aziendali è consentito solo al personale autorizzato, tramite identificazione univoca dell'utente;
- gli accessi agli applicativi aziendali, così come alle cartelle di rete, sono profilati sulla base della posizione ricoperta;
- con specifico riferimento ai sistemi informativi aziendali, le abilitazioni di accesso e la relativa profilazione, così come ogni operazione di cancellazione o modifica delle utenze, possono essere richieste esclusivamente dall'Identity Manager secondo competenza;
- il riconoscimento dell'utente avviene attraverso username e password. Al dipendente neo assunto viene attribuita una password provvisoria da modificarsi al primo log-on;
- la comunicazione delle password di accesso agli applicativi aziendali avviene in modalità confidenziale ed è cura di ogni dipendente la custodia e non divulgazione della stessa;
- i sistemi richiedono automaticamente un aggiornamento delle password di accesso ogni 90 giorni;
- sono effettuate attività periodiche di monitoraggio degli accessi agli applicativi aziendali e revisioni delle utenze attive al fine di garantire la corretta profilazione e concessione dei privilegi a sistema;
- ogni dipendente è dotato di indirizzo di posta elettronica nominativo ad esclusivo uso lavorativo.

Gestione dei Back-up

- La Società dispone di piani di backup periodico dei dati, file, programmi e sistemi operativi, al fine di garantire la salvaguardia del patrimonio informativo aziendale;
- il backup dei dati è effettuato mediante supporti rimovibili;
- sono effettuati test di restore periodici.

Gestione di software, apparecchiature, dispositivi o programmi informatici

- Le postazioni di lavoro sono dotate esclusivamente di software con regolare licenza;
- non è consentito scaricare software di alcun tipo sulle postazioni di lavoro.

Gestione della sicurezza della rete

- Server e client sono dotati di software antivirus aggiornati automaticamente;
- il server di posta elettronica è dotato di filtri antispamming, anti phishing e antivirus;
- l'accesso ad internet è filtrato tramite un sistema automatico di web filtering.

Gestione della sicurezza fisica

- La gestione della sala CED è di competenza della Funzione IT di Corporate;
- l'accesso alla sala CED è garantito solo a personale autorizzato ed è monitorato mediante la compilazione di un registro delle entrate.