**Caterpillar Fluid Systems S.r.l.**

# Modello di organizzazione, gestione e controllo

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

## *Parte Speciale F*

## *Gestione dei sistemi informativi*

Documento approvato dal Consiglio di Amministrazione

con delibera del 24.09.2024

## 1 FINALITÀ

La presente Parte Speciale del Modello ha la finalità di definire le regole che tutti i Destinatari coinvolti nell'ambito dell'Attività Sensibile identificata nel successivo paragrafo 2 devono osservare al fine di prevenire la commissione dei reati previsti dal D.Lgs. 231/2001 e 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 e i presidi di controllo che gli esponenti aziendali devono osservare ai fini della corretta applicazione del Modello;
- fornire all'Organismo di Vigilanza ed alle altre strutture di controllo gli strumenti per esercitare le attività di monitoraggio, controllo, verifica.

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

- Parte Generale del Modello;
- Codice di Condotta e Politiche Aziendali del Gruppo Caterpillar;
- Sistema di procure e deleghe in vigore;
- ogni altro documento aziendale (ivi incluse le Procedure Corporate, le Procedure Interne e, per quanto applicabili, le Procedure SOX) 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 GESTIONE DEI SISTEMI INFORMATIVI

### *2.1. I reati potenzialmente rilevanti*

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

- i reati informatici e di trattamento illecito dei dati richiamati dall'art. 24-*bis* del D.Lgs. 231/01, in particolare:
  - falsità in un documento informatico pubblico o privato;
  - accesso abusivo ad un sistema informatico o telematico;
  - detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici;
  - danneggiamento di informazioni, dati e programmi informatici;
  - danneggiamento di sistemi informatici o telematici;

  - diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico;
  - intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche;
  - danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità;
  - danneggiamento di sistemi informatici o telematici di pubblica utilità;
- i reati in materia di violazione del diritto d'autore richiamati dall'art. 25-*novies* del D.Lgs. 231/01, in particolare:
  - abusiva duplicazione, detenzione e diffusione, al personale della Società o a fornitori, di software non licenziati, al fine di ottenere un vantaggio economico;
  - abusiva duplicazione, detenzione da personale della Società o da fornitori di contenuti multimediali/disegni protetti dal diritto d'autore;
- i reati contro la Pubblica Amministrazione richiamati dagli art. 24 e 25 del D.Lgs. 231/2001, in particolare:
  - frode informatica.

### *2.2. Ambito di applicazione*

I successivi principi di comportamento e presidi di controllo si applicano a tutti i Destinatari coinvolti nelle attività relative alla gestione dei sistemi informativi e, in particolare, ma non esclusivamente, a:

- Responsabili dei sistemi informativi riferiti alla società Caterpillar Fluid Systems - Italia

### *2.3. Principi di comportamento da adottare*

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

- valutare la corretta implementazione tecnica delle abilitazioni / profilazioni utente ai principali sistemi aziendali, verificandone la corrispondenza con le mansioni indicate dai Responsabili di ciascuna Funzione ed il rispetto del principio generale di segregazione dei compiti;
- monitorare il corretto utilizzo degli accessi (*user-id*, *password*) ai sistemi informativi aziendali e di terze parti;
- verificare la sicurezza della rete e dei sistemi informativi aziendali e tutelare la sicurezza dei dati;
- identificare le potenziali vulnerabilità nel sistema dei controlli IT;
- prevedere un processo di *change management* segregato con la finalità di ridurre al minimo attività di danneggiamento dei sistemi informatici;
- verificare la sicurezza fisica e dei sistemi informativi aziendali e tutelare la sicurezza dei dati;

- monitorare il corretto utilizzo degli accessi fisici ai sistemi informativi di dipendenti e terze parti;
- vigilare sulla corretta applicazione di tutti gli accorgimenti ritenuti necessari al fine di fronteggiare, nello specifico, i delitti informatici e il trattamento illecito dei dati, suggerendo ogni più opportuno adeguamento;
- monitorare le attività di fornitori terzi in materia di *networking*, gestione degli applicativi e gestione dei sistemi *hardware*;
- garantire che non sia consentito l'accesso alle aree riservate (quali *server rooms*, locali tecnici, ecc.) alle persone che non dispongono di idonea autorizzazione, temporanea o permanente e, in ogni caso, nel rispetto della normativa (interna ed esterna) vigente in materia di tutela dei dati personali.

Inoltre, tutti i dipendenti della Società devono:

- utilizzare gli strumenti informatici aziendali e assegnati nel rispetto delle procedure aziendali in vigore ed esclusivamente per l'espletamento della propria attività lavorativa;
- utilizzare la navigazione in internet e la posta elettronica esclusivamente per le attività lavorative;
- custodire accuratamente le proprie credenziali d'accesso ai sistemi informativi utilizzati, evitando che soggetti terzi possano venirne a conoscenza, e aggiornare periodicamente le *password*;
- custodire accuratamente le risorse informatiche aziendali o di terze parti (es. *personal computer* fissi o portatili) utilizzate per l'espletamento delle attività lavorative;
- rispettare le *policy* di sicurezza concordate e definite con le terze parti per l'accesso a sistemi o infrastrutture di queste ultime.

È infine espressamente vietato:

- detenere, diffondere o utilizzare abusivamente codici di accesso a sistemi informatici o telematici di terzi o di enti pubblici;
- distruggere o alterare documenti informatici archiviati sulle *directory* di rete o sugli applicativi aziendali e, in particolare, i documenti che potrebbero avere rilevanza probatoria in ambito giudiziario;
- lasciare documenti incustoditi contenenti informazioni riservate o codici di accesso ai sistemi;
- porre in essere condotte, anche con l'ausilio di soggetti terzi, miranti all'accesso a sistemi informativi altrui con l'obiettivo di acquisire abusivamente, danneggiare o distruggere informazioni o dati contenuti nei suddetti sistemi informativi;
- danneggiare, distruggere gli archivi o i supporti relativi all'esecuzione delle attività di back-up;
- lasciare incustodito il proprio personal computer sbloccato;
- utilizzare i sistemi informativi a disposizione per attività non autorizzate nell'ambito dell'espletamento delle attività lavorative;
- acquisire abusivamente, danneggiare o distruggere informazioni o dati contenuti nei sistemi informativi aziendali o di terze parti;

- entrare nella rete aziendale e nei programmi con un codice d'identificazione utente diverso da quello assegnato;
- rivelare ad alcuno le proprie credenziali di autenticazione (nome utente e password) alla rete aziendale o anche ad altri siti/sistemi;
- aggirare o tentare di eludere i meccanismi di sicurezza aziendali (Antivirus, Firewall, Proxy Server,) ecc.) di terze parti;
- porre in essere condotte miranti alla distruzione o all'alterazione di sistemi informativi aziendali o di terze parti;
- intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche;
- salvare sulle unità di memoria aziendali contenuti o file non autorizzati o in violazione del diritto d'autore;
- utilizzare o installare programmi diversi da quelli autorizzati dal Direttore Sistemi Informativi e privi di licenza;
- installare, duplicare o diffondere a terzi programmi (software) senza essere in possesso di idonea licenza o superando i diritti consentiti dalla licenza acquistata (es. numero massimo di installazioni o di utenze);
- alterare in qualsiasi modo il funzionamento di un sistema informatico o telematico della Pubblica Amministrazione, o intervenire senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico della Pubblica Amministrazione, al fine di procurare un vantaggio per la Società;
- accedere ad aree riservate (quali server rooms, locali tecnici, ecc.) senza idonea autorizzazione, temporanea o permanente.

### *2.4. Presidi di controllo da applicare*

Nella gestione delle attività in oggetto, tutti i Destinatari coinvolti dovranno conformarsi a quanto previsto dalle Procedure Corporate e Procedure Interne.

Premesso che tutti i controlli previsti dalle suddette Procedure devono essere pienamente garantiti, qui di seguito sono indicati i presidi di controllo ritenuti maggiormente rilevanti al fine di mitigare potenziali rischi-reato ai sensi del D.Lgs. 231/2001.

- Tramite appositi contratti di Service Agreement, le società del Gruppo Caterpillar prestano servizi nei confronti di Caterpillar Fluid Systems in ambito di gestione dei sistemi informativi. Tali contratti sono validati da parte di soggetti dotati di idonei poteri sulla base del sistema di deleghe e procure in essere.

#### *2.4.1 Gestione profili e password*

- Le attività di gestione degli accessi a dati e sistemi sono gestite esternamente da società del Gruppo Caterpillar; per quanto afferente alcuni software locali, oltre a quanto riportato precedentemente, la gestione è in carico alla Funzione IT locale.
- L'accesso ai sistemi informativi aziendali è consentito solo al personale autorizzato. L'accesso agli applicativi aziendali è profilato sulla base della funzione di pertinenza di ciascun utente. Gli accessi sono autorizzati dal responsabile di settore.
- Il Responsabile della Direzione Personale e Organizzazione comunic, in caso di nuove assunzioni, dismissioni o modifiche di mansioni, alla Funzione IT le richieste di apertura /modifica/ chiusura di utenze.
- Sono individuati gli utenti con diritti di amministratore di sistema.
- Le password di dominio e degli applicativi sono debitamente configurate secondo Procedure Corporate.
- Al primo *log-on* è richiesto all'utente il cambio password obbligatorio.
- Sono previsti blocchi di sistema in caso di errata digitazione della password (dopo tre tentativi errati) e blocchi di inattività.
- Viene tenuta traccia dei log a sistema dell'ultima operazione eseguita dall'utente.

*2.4.2 Gestione back-up*

- Le attività di backup sono gestite esternamente da altre società del Gruppo Caterpillar.
- Tutte le informazioni aziendali che risiedano sui server e sulle banche dati centrali devono essere sottoposte a *backup* giornaliero automatico.
- Periodicamente sono eseguite in automatico attività per la verifica del corretto esito del *backup*.
- Annualmente viene effettuato un test di *disaster recovery*.
- Esiste una procedura che disciplina le attività di test di *restore* per verificare l'integrità dei supporti di backup.
- I supporti di backup sono conservati in armadi chiusi a chiave accessibili esclusivamente al personale abilitato.

*2.4.3 Gestione di software, apparecchiature, dispositivi o programmi informatici*

- Le postazioni di lavoro sono dotate esclusivamente di software con licenza.
- Non è consentito installare *software* di alcun tipo sui dispositivi aziendali.
- Il responsabile dell'area Sistemi Informativi detiene una lista dei *software* installati sulle postazioni di lavoro e la aggiorna periodicamente (mappatura licenze). Le eventuali eccezioni/anomalie vengono tempestivamente indagate.

*2.4.4 Gestione della sicurezza di rete*

- Le attività di garanzia della sicurezza della rete sono gestite da CAT Security.
- La rete è protetta da *firewalls*.
- La rete di trasmissione di dati aziendale è protetta contro il rischio di accesso abusivo tramite adeguati strumenti di monitoraggio, gestiti centralmente da CAT Security.
- L'accesso ad internet è filtrato tramite un sistema di *web filtering* e *firewall*.
- *Server e client* sono dotati di sistemi antivirus aggiornati automaticamente.
- La posta elettronica è filtrata in ingresso da sistemi antispam e antivirus. Sono inoltre previsti dei limiti sulla dimensione degli allegati.
- L'accesso ai dati e la creazione degli Share Folder sono gestiti centralmente da CAT Security per mezzo dello strumento FAM (Folder Access Management) oltre all'uso di user ID/password per l'accesso al sistema.

*2.4.5 Gestione della sicurezza fisica*

- L'accesso ai Data Center è consentito al solo personale autorizzato.
- Il personale non abilitato all'accesso alla sala CED deve essere accompagnato dal personale autorizzato.