

# **B21 FACILITY MANAGEMENT SOCIETA' COOPERATIVA**

## **Modello di Organizzazione, Gestione e Controllo ex D.Lgs. n. 231/2001**

### **Parte Speciale "F"**

**"Delitti informatici e trattamento illecito dei dati, Delitti in materia di  
violazione del diritto d'autore"  
(Articoli 24-*bis* del Decreto)**

## Sommario

Parte Speciale “F” .....	1
1    Finalità .....	4
2    Reati .....	4
3    I processi sensibili ai fini del D.Lgs. n. 231/01 .....	5
4    Divieti .....	6
5    Principi generali di controllo .....	6
6    Protocolli specifici di comportamento e controllo per attività sensibili individuate .....	8
6.1    Acquisizione delle commesse, erogazione e valutazione dei servizi .....	8
6.2    Gestione IT .....	9

### Indice delle Revisioni

Revisione	Approvazione	Natura delle modifiche
Rev. 00	Consiglio di amministrazione del 11.10.2022	Adozione

## 1 Finalità

La Parte Speciale F del Modello organizzativo ex D.Lgs. n. 231/01 ha la finalità di delineare i principi generali di controllo e i protocolli specifici di comportamento e controllo che i soggetti coinvolti nell’ambito dei processi sensibili, indicati nel successivo paragrafo 3, dovranno seguire al fine di prevenire la commissione dei reati presupposto del D.Lgs. n. 231/01 riportati nel prossimo paragrafo e di assicurare condizioni di correttezza e trasparenza nella conduzione delle attività dell’ente.

La presente Parte Speciale ha il fine di:

- evidenziare le regole che devono essere osservate ai fini della corretta applicazione del Modello;
- fornire alle altre funzioni di controllo e, in particolare, all’organismo di Vigilanza gli strumenti per esercitare le attività di monitoraggio, controllo, verifica.

Gli esponenti aziendali devono avere, ciascuno per gli aspetti di propria competenza, comportamenti conformi al contenuto dei seguenti documenti:

- Modello Organizzativo
- Codice Etico
- Procedure interne
- Procure e deleghe
- Protocolli e principi di comportamento riferiti alle specifiche aree aziendali
- Ogni altro documento che regoli attività rientranti nell’ambito di applicazione del Decreto.

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

## 2 Reati

Si riporta di seguito l’elenco dei reati richiamati dall’art. 24-bis del D.Lgs. n. 231/01.

### Art. 24-bis

- Accesso abusivo ad un sistema informatico o telematico (Art. 615-ter c.p.)
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (Art. 617-quater c.p.)
- Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (Art. 617-quinquies 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.)
- 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.)
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (Art. 615-quater c.p.)
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (Art. 615-quinquies c.p.)
- Falsità in un documento informatico (Art. 491-bis c.p.)
- Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (Art. 640-quinquies c.p.)

Per la descrizione di ciascuna fattispecie di reato si rinvia all’Allegato “**Tabella reati/illeciti presupposto della responsabilità EX D.LGS. 231/01**” del Modello.

### 3 I processi sensibili ai fini del D.Lgs. n. 231/01

I processi sensibili, ossia i processi più specificatamente a rischio di commissione dei reati societari sono ritenute essere le seguenti:

#### 1. **Acquisizione ed esecuzione delle commesse**

L'azienda si occupa come attività principale dei trasporti.

[OMISSIS] L'azienda lavora con la PA dalla quale riceve commesse. Quando l'azienda acquisisce una commessa deve essere messo in atto quanto previsto dalla normativa vigente relativamente alla cooperazione e al coordinamento delle misure di prevenzione e protezione dai rischi derivanti dall'attività lavorativa oggetto dell'appalto. Ad ogni appalto assegnato e prima dell'inizio dei rispettivi lavori in cantiere, B 21 invia o consegna *brevi manu* il POS e la documentazione richiesta dal Committente nel contratto stesso; in aggiunta il Responsabile della Qualità, supportato dal Direttore Tecnico provvede a reperire presso l'ente appaltante, ove non già presente nella documentazione a corredo dell'appalto le informazioni utili alla corretta gestione ambientale e di sicurezza.

#### 2. **Gestione IT**

Il processo in esame concerne le attività sensibili di gestione e manutenzione delle risorse informatiche

[OMISSIS] La società non gestisce particolari dati sensibili, fatta eccezione per quelli dei dipendenti. Nei dispositivi informatici aziendali non vengono installati software o applicazioni ad uso personale dei dipendenti. Inoltre, si utilizzano i dispositivi aziendali per le mail e le comunicazioni tra uffici o comunque relative alle attività della società. I PC sono dotati di psw e utente per l'accesso. Ogni soggetto ha proprie credenziali per l'accesso al proprio pc che conosce solo lui e cambia con cadenza semestrale. Ogni operatore accede unicamente ai propri sistemi informatici di competenza e utilizza la propria mail unicamente dal proprio personal computer. La pec viene gestita solo dal Presidente e da operatori espressamente autorizzati

## 4 Divieti

La presente Parte Speciale prevede, coerentemente con i principi del Codice Etico, l'espresso divieto per i Destinatari di:

- utilizzare le risorse informatiche (es. PC fissi o portatili) assegnate per finalità diverse da quelle lavorative;
- porre in essere condotte, anche con l'ausilio di soggetti terzi, miranti all'accesso a sistemi informativi altrui con l'obiettivo di:
  - acquisire abusivamente informazioni contenute nei suddetti sistemi informativi;
  - danneggiare, distruggere dati contenuti nei suddetti sistemi informativi;
  - utilizzare abusivamente codici d'accesso a sistemi informatici e telematici nonché procedere alla diffusione degli stessi;
- distruggere o alterare documenti informatici archiviati sulle *directory* di rete o sugli applicativi aziendali se non dietro autorizzazione;
- utilizzare o installare programmi diversi da quelli autorizzati dall'ente;
- aggirare o tentare di aggirare i meccanismi di sicurezza aziendali (*antivirus, firewall, ecc.*);
- rivelare ad alcuno le proprie credenziali di autenticazione (nome utente e *password*) alla rete aziendale o anche ad altri siti/sistemi;
- intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche;
- rilevanza probatoria in ambito giudiziario;
- alterare o falsificare documenti informativi di qualsiasi natura;
- utilizzare in modo improprio gli strumenti di firma digitale assegnati;
- 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;
- entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato;
- installare, duplicare o diffondere a terzi programmi (*software*) senza essere in possesso di idonea licenza.

## 5 Principi generali di controllo

Tutte le attività sensibili devono essere gestite nel rispetto dei seguenti principi generali di controllo:

- principi etico-comportamentali disciplinati nella presente Parte Speciale e nel Codice Etico di B21 fm società cooperativa;
- regolamentazione interna e protocolli specifici di comportamento e di controllo: si tratta di regole formali o prassi consolidate idonee a definire ruoli, responsabilità, modalità operative e attività di controllo cui attenersi per lo svolgimento delle attività dell'ente, ivi incluse quelle più sensibili.

In particolare, i principi generali di controllo posti a base degli strumenti e delle metodologie utilizzate per strutturare i presidi specifici di controllo possono essere sintetizzati come segue:

- **esistenza di procedure** che disciplinino formalmente gli aspetti relativi a:
  - ruoli responsabili del processo sensibile;
  - modalità operative del processo;
  - documentazione da produrre nelle varie fasi in cui è articolato il processo;
  - flussi di comunicazione tra i soggetti coinvolti nelle attività in cui è articolato il processo.
- **tracciabilità**: ogni transazione deve essere documentata in modo da consentirne la verificabilità ex post con un adeguato livello di formalizzazione (flussi informativi); in particolare: 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;
- **segregazione**: 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, all'interno di ciascun processo sensibile, le attività di esecuzione, controllo e autorizzazione devono essere assegnate a soggetti diversi tra loro;
- **esistenza di un sistema di deleghe e procure** coerente con le responsabilità organizzative assegnate: formalizzazione di strumenti di delega e/o esistenza di strumenti idonei, che forniscano una chiara descrizione di ruoli e responsabilità (es. mansionario) dei soggetti coinvolti nel processo sensibile.

Si intende per “delega” quell’atto interno di attribuzione di funzioni e compiti, riflesso nel sistema di comunicazioni organizzative. Si intende per “procura” il negozio giuridico unilaterale con cui B21 fm società cooperativa attribuisce ad un singolo soggetto il potere di agire in rappresentanza della stessa. I requisiti essenziali per il rilascio di deleghe e procure sono i seguenti:

- tutti coloro che intrattengono per conto della società rapporti con la P.A., devono essere dotati di delega formale in tal senso;
- le deleghe devono coniugare ciascun potere alla relativa responsabilità e ad una posizione adeguata nell’organigramma;
- ciascuna delega deve definire in modo specifico ed inequivocabile:
  - i poteri del delegato, precisandone i limiti;
  - il soggetto (organo o individuo) cui il delegato riporta gerarchicamente;
- al delegato devono essere riconosciuti poteri di spesa adeguati alle funzioni conferite;
- a ciascuna procura che comporti il potere di rappresentanza dell’ente nei confronti dei terzi deve corrispondere una delega interna che descriva il relativo potere di gestione;
- la procura deve prevedere esplicitamente i casi di decadenza dai poteri conferiti (revoca, trasferimento a diverse mansioni incompatibili con quelle per le quali la procura era stata conferita, chiusura del rapporto dipendente, ecc.);
- le deleghe e le procure devono essere tempestivamente aggiornate.

L’O.d.V. verifica periodicamente, con il supporto degli uffici competenti, il sistema di deleghe e procure in vigore e la loro coerenza con tutto il sistema delle comunicazioni organizzative e delle procedure, raccomandando eventuali modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti al delegato o vi siano altre anomalie.

L’O.d.V. verifica periodicamente le attività svolte in outsourcing.

## 6 Protocolli specifici di comportamento e controllo per attività sensibili individuate

### 6.1 Acquisizione delle commesse, erogazione e valutazione dei servizi

#### Attività sensibili e responsabili del processo

[Si rimanda a quanto descritto nella *Parte Speciale A “Reati contro la Pubblica Amministrazione”*]

#### Principi etico-comportamentali

[Si rimanda a quanto descritto nella *Parte Speciale A “Reati contro la Pubblica Amministrazione”*]

#### Principi di comportamento e di controllo specifici

[Si rimanda a quanto descritto nella *Parte Speciale A “Reati contro la Pubblica Amministrazione”*]



## 6.2 Gestione IT

### Attività sensibili e responsabili del processo

Nell'ambito del processo sensibile possono essere considerate alcune attività sensibili quali la Gestione profilatura utenti e processo di autenticazione, Gestione e protezione dell'integrità delle informazioni, Gestione dei software, apparecchiature, dispositivi e programmi informatici, Gestione sicurezza della rete, Gestione della sicurezza fisica e ambiente.  
È responsabile del processo il Presidente della cooperativa.

### Principi etico-comportamentali

Fatti salvi i divieti di cui al paragrafo 4, tutti i Destinatari del presente Modello che abbiano accesso a dispositivi e programmi informatici di B21fm devono:

- utilizzare le risorse informatiche assegnate esclusivamente per l'espletamento della propria attività;
- utilizzare le risorse informatiche messe a disposizione dei partner seguendo le specifiche direttive ed indicazioni di questi ultimi;
- utilizzare gli strumenti informatici nel rispetto delle procedure definite;
- custodire accuratamente le proprie credenziali d'accesso ai sistemi informativi utilizzati, evitando che terzi soggetti possano venirne a conoscenza e aggiornare periodicamente le *password*.

Inoltre, le funzioni preposte alla gestione dei sistemi informativi, devono:

- verificare la sicurezza della rete e dei sistemi informativi e tutelare la sicurezza dei dati;
- identificare le potenziali vulnerabilità nel sistema dei controlli informatici;
- monitorare l'infrastruttura tecnologica al fine di garantirne la manutenzione e la sicurezza fisica;
- garantire la manutenzione software e hardware dei sistemi;
- 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 la sicurezza del sistema informativo.

Le attività eventualmente svolte da parte di fornitori terzi in materia di:

- gestione degli applicativi,
- gestione dei sistemi *hardware*,

devono rispettare i principi e le regole stabilite dall'ente, al fine di tutelare la sicurezza dei dati ed il corretto accesso da parte dei soggetti ai sistemi applicativi ed infrastrutturali.

Infine, le attività devono essere svolte conformemente ai principi esposti nel Codice Etico.

### Principi di comportamento e di controllo specifici

Le attività di (i) gestione profilatura utenti e processo di autenticazione; (ii) gestione e protezione dell'integrità delle informazioni; (iii) gestione di software, apparecchiature, dispositivi programmi informatici; (iv) gestione della sicurezza della rete e (v) gestione della sicurezza fisica e ambiente, devono essere regolamentate in modo da identificare le responsabilità dei soggetti coinvolti, le modalità operative e di controlli che devono essere svolti.

Quali misure che si suggerisce di attuare per evitare o ridurre rischi in materia di privacy, si evidenziano le seguenti:

- Modifica periodica delle credenziali
- Attuazione di Backup di file e programmi ed eventualmente attuazione di copie multiple di backup
- Sistema di autenticazione per l'accesso alle banche dati
- Impiego di firewall
- Impiego di antivirus
- Manutenzione periodica degli strumenti HW/SW
- Protezione dei locali dall'accesso di non addetti
- Eventuale impiego di gruppi continuità

In particolare, le procedure, le policy e le prassi vigenti devono garantire il rispetto dei seguenti Protocolli specifici di comportamento e di controllo, essendo suggerito:

- rispettare e assumere tutte le necessarie azioni richieste dalla normativa vigente in materia di privacy;

- adottare procedure formali per la gestione delle risorse e dei processi tecnologici;
- rendere tracciabile ogni comunicazione ed ogni informazione che passino attraverso risorse IT;
- adottare una segregazione di ruoli, specialmente tra chi assume decisioni in merito alla gestione dei processi e delle risorse tecnologici, chi ne controlla il funzionamento, chi verifica il rispetto delle normative legate a tali risorse;
- impiegare un sistema di deleghe e strumenti che individuino formalmente ruoli e responsabilità dei membri dell'ente nella gestione delle risorse IT.

Di seguito si evidenziano dei suggerimenti per un'efficace e sicura gestione delle risorse tecnologiche nell'ambito di ogni attività sensibile rilevata:

**a) Gestione profilatura utenti e processo di autenticazione**

- l'accesso alle informazioni che risiedono sui server e sulle banche dati, dovrebbe essere limitato da idonei strumenti di autenticazione;
- gli amministratori di sistema, gli addetti alla manutenzione e gli incaricati della società dovrebbero essere muniti di univoche credenziali di autenticazione, con caratteristiche di sicurezza almeno equipollenti a quelle previste dalla vigente normativa e prassi sulla privacy; le credenziali di autenticazione devono essere mantenute segrete;
- dovrebbe essere definita una procedura di registrazione e rimozione per accordare o revocare l'accesso a tutti i sistemi e servizi informativi;
- l'attivazione o la modifica di un profilo utente deve essere autorizzata;
- deve essere disciplinata la rimozione dei diritti di accesso in caso di cessazione o cambiamento dei tipi di rapporto che attribuiva il diritto di accesso;
- l'aggiornamento delle password dei singoli utenti sui diversi applicativi deve essere garantito dall'applicazione di regole specifiche;
- l'accesso tramite VPN deve essere consentito tramite nome utente e password.

**b) Gestione e protezione dell'integrità delle informazioni**

- ciascun utente ha l'accesso limitato, attraverso una propria profilatura, a sezioni specifiche dei database, che viene definita in relazione al tipo di mansione e all'area di attività corrispondente;
- deve essere garantita la chiusura di sessioni inattive dopo un predefinito periodo di tempo;
- tutte le informazioni aziendali che risiedono sui server, sulle banche dati centrali, sono sottoposti a regolare procedura di *backup*; si deve assicurare che le procedure di salvataggio siano adeguate e provvedere al corretto mantenimento dei file di log generati dai sistemi;
- il responsabile del processo dovrebbe effettuare il salvataggio periodico dei dati e la relativa archiviazione;
- il responsabile del processo dovrebbe effettuare attività di verifica dell'effettiva esecuzione delle attività di *backup*;
- il responsabile del processo dovrebbe garantire la corretta attribuzione/abilitazione degli accessi a siti o programmi di terzi (enti pubblici o privati) che richiedano credenziali di accesso (user-id, password, smart card);
- devono essere implementate soluzioni di Disaster Recovery.

**c) Gestione di software, apparecchiature, dispositivi o programmi informatici**

- deve essere assicurato l'aggiornamento periodico di tutti i sistemi in linea con gli aggiornamenti messi a disposizione dai produttori di software;
- tutti i programmi installati sulle postazioni di lavoro devono essere dotati di licenza;
- il responsabile del processo, anche servendosi di personale competente, dovrebbe effettuare una verifica annuale dei software presenti sulle postazioni dei vari utenti, rimuovendo i software vietati o privi di licenza.

**d) Gestione della sicurezza della rete**

- la rete di trasmissione dati aziendali deve essere protetta da adeguati strumenti di limitazione degli accessi (firewall);
- i server e le postazioni fisse e portatili devono essere protetti contro potenziali attacchi esterni attraverso l'utilizzo di software antivirus, che effettua controlli in entrata e in uscita, costantemente aggiornati;

- il responsabile IT deve effettuare una verifica annuale dei software installati sui pc collegati alla rete aziendale.
- e) Gestione della sicurezza fisica e ambiente***
- i Data Center dovrebbero essere localizzati in ambienti che ne garantiscono la sicurezza fisica e accessibili a personale autorizzato.