

Modello di Organizzazione, Gestione e Controllo
ex Decreto Legislativo 8 giugno 2001 n. 231

PARTE SPECIALE "B"

REATI INFORMATICI E REATI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE

MATRICE DEL DOCUMENTO		
Adottato dall'Amministratore Unico	Data	Firma

INDICE

REATI INFORMATICI **1**
E **1**
REATI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE **1**

1. Reati informatici e reati in materia di violazione del diritto d'autore. **3**

1.1 Premessa **3**

1.2 Rinvio al catalogo dei reati **3**

2. Fattispecie di attività sensibili in relazione ai reati informatici e ai reati in materia di violazione del diritto d'autore **3**

3. Funzioni coinvolte **4**

4. Procedure e programmi applicabili **4**

5. Regole generali di comportamento – reati informatici e in materia di violazione del diritto d'autore. **4**

6. Principi di controllo specifici – reati informatici e in materia di violazione del diritto d'autore **5**

6.1 Gestione della sicurezza fisica e logica dei sistemi informativi **5**

6.2 Gestione e protezione delle reti informatiche aziendali **6**

6.3 Gestione e sviluppo di programmi applicativi di proprietà di terzi **7**

6.4 Gestione degli output di sistema e dei dispositivi di memorizzazione **7**

7. Controlli dell'Organismo di Vigilanza **8**

1. Reati informatici e reati in materia di violazione del diritto d'autore.

1.1 Premessa

La prevenzione dei reati informatici, contemplati all'art. 24-bis[1], nonché dei reati connessi alla violazione del diritto d'autore contemplati dall'art. 25-novies[2] del D.lgs. 231/2001, viene di seguito rappresentata in maniera unitaria, stante l'omogeneità degli interessi tutelati dalle norme incriminatrici, delle aree di rischio.
Inoltre, va tenuto conto che l'eventuale condanna di uno o più operatori aziendali per una delle fattispecie di reato considerate dagli artt. 24-bis e 25-novies del Decreto 231 può comportare la punibilità dell'Azienda - sempre a condizione che abbia avuto interesse o comunque tratto vantaggio dall'attività criminosa - non solo in termini di sanzioni pecuniarie, ma anche con le più pesanti sanzioni interdittive previste dall'art. 9 del Decreto [3].

1.2 Rinvio al catalogo dei reati

Ai fini di una migliore comprensione della normativa in tema di responsabilità degli enti da reato di cui alla presente Parte Speciale si rinvia alla lettura estesa dei reati informatici e trattamento illecito di dati contemplati agli articoli 24-bis del d.lgs. 231/2001, e dei delitti in materia di violazione del diritto d'autore di cui all'art. 25-novies del d.lgs. 231/2001, i quali vanno contemplati anche tenendo conto della fattispecie del concorso di persone nel reato (art. 110 c.p.).

2. Fattispecie di attività sensibili in relazione ai reati informatici e ai reati in materia di violazione del diritto d'autore

In considerazione dei processi aziendali di seguito vengono individuate le fattispecie di attività sensibili al rischio dei reati in esame:

- ✓ **gestione della sicurezza fisica e logica dei sistemi informativi;**
- ✓ **gestione e protezione delle reti informatiche aziendali;**
- ✓ **gestione e sviluppo di programmi applicativi di proprietà di terzi;**
- ✓ **gestione degli output di sistema e dei dispositivi di memorizzazione;**
- ✓ **gestione dei sistemi di business continuity (sistemi di backup e disaster recovery);**
- ✓ **gestione del firewall e dei sistemi antivirus;**
- ✓ **verifica delle licenze per l'utilizzo di software;**
- ✓ **Gestione, sviluppo e manutenzione software;**
- ✓ **Attività di creazione, protezione, emissione, archiviazione, conservazione, eliminazione, divulgazione, immissione in reti informatiche/telematiche di documenti informatici e manutenzione in genere degli archivi di documenti informatici;**
- ✓ **Attività di trasmissione di dati ed informazioni alle pubbliche autorità.**

Di seguito sono formalizzate, in relazione alle predette fattispecie, le funzioni aziendali coinvolte, le procedure di riferimento, le regole generali di comportamento ed i principi di controllo applicabili nell'organizzazione e gestione delle attività di volta in volta disimpegnate.

---

[1] Tale articolo è stato introdotto nel Decreto 231 dall'art. 7 della legge n. 48/2008 di ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno.

[2] Tale articolo è stato introdotto nel Decreto dall'art. 15, comma 7, lett. c) della legge n. 99/2009 recante "disposizioni per lo sviluppo e l'internazionalizzazione delle imprese".

3 L'art. 24-bis, comma 4, del Decreto prevede anche una gradazione nell'applicabilità di determinate sanzioni interdittive piuttosto che altre, in ragione delle diverse fattispecie di delitti informatici per i quali si procede.

3. Funzioni coinvolte

Di seguito, si evidenziano le funzioni aziendali coinvolte nelle fattispecie di attività sensibili sopra riportate:

- Amministratore Unico;
- Direttore Generale;
- Direttore Tecnico;
- Responsabile Amministrativo;
- Architetto.

Per quanto attiene all'identificazione delle attività sensibili sono state individuate le seguenti aree di attività "sensibili" a rischio:

1. Gestione delle attività di accesso ai sistemi informatici/telematici e applicazioni (autenticazione, account e profili);
2. Gestione dell'attività di elaborazione dei dati;
3. Attività di manutenzione dei sistemi informatici/telematici e di accesso alle applicazioni;
4. Gestione e manutenzione hardware;
5. Gestione, sviluppo e manutenzione software;
6. Gestione degli accessi fisici ai locali in cui sono localizzati i sistemi e le infrastrutture IT;
7. Attività di creazione, protezione, emissione, archiviazione, eliminazione, divulgazione, immissione in reti informatiche/telematiche di documenti informatici e manutenzione in genere degli archivi di documenti informatici;
8. Attività di trasmissione di dati ed informazioni alle pubbliche autorità;
9. Gestione della sicurezza informatica.

4. Procedure e programmi applicabili

Di seguito si evidenziano gli atti societari e le procedure aziendali vigenti che hanno impatto diretto o indiretto sulla prevenzione dei reati *de quibus* ed incidono sulla regolamentazione delle fattispecie di attività sensibili riportate:

ELENCO PROCEDURE CHE FORMALIZZANO RUOLI E RESPONSABILITÀ COINVOLTI NELLE ATTIVITA' SENSIBILI RELATIVE AI REATI INFORMATICI
Partizione sistemi informativi e relative procedure gestionali.
Mappatura software e licenze aziendali.
Manuale GDPR – Sistema di gestione Privacy

5. Regole generali di comportamento – reati informatici e in materia di violazione del diritto d'autore.

I soggetti apicali di Berna Engineering S.r.l. (amministratore, gestori di fatto, ecc.), nonché le persone sottoposte alla loro vigilanza, sono tenuti ad osservare nelle fattispecie di attività sensibili sopra delineate, nonché nella sfera dei rapporti societari in genere, le seguenti regole di condotta. Più precisamente, quanto alla prevenzione dei ***reati informatici***, è fatto obbligo di:

- ✓ fornire, ai destinatari, un'adeguata informazione relativamente al corretto utilizzo delle risorse informatiche aziendali ed al rischio della commissione di Reati informatici;
- ✓ limitare l'accesso a reti e sistemi informatici esterni alla società compatibilmente con le necessità lavorative;

- ✓ effettuare controlli periodici sulla rete informatica aziendale al fine di individuare comportamenti anomali quali, a titolo di esempio, il download di files di grosse dimensioni, ovvero attività eccezionali dei *server* al di fuori degli orari di operatività sociale.

È pertanto assolutamente vietata la trasmissione di qualsiasi atto non veritiero, contraffatto o non autentico attraverso un invio telematico.

Per quanto attiene alla prevenzione dei ***reati in materia di violazione del diritto d'autore***, è fatto obbligo di:

- ✓ informare gli utilizzatori dei sistemi informatici che il software loro assegnato è protetto dalle leggi sul diritto d'autore ed in quanto tale ne è vietata la duplicazione, la distribuzione, la vendita o la detenzione a scopo commerciale/imprenditoriale;
- ✓ adottare regole di condotta aziendali che riguardino tutto il personale della Società nonché i terzi che agiscono per conto di quest'ultima;
- ✓ fornire, ai destinatari, un'adeguata informazione relativamente alle opere protette dal diritto d'autore ed al rischio della commissione di tale reato.

In entrambi i casi, è fatto divieto di:

- ✓ porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (artt. 24-bis e 25-novies del D.Lgs. 231/2001);
- ✓ violare i principi e le procedure aziendali già vigenti in materia previste nella presente sezione.

6. Principi di controllo specifici – reati informatici e in materia di violazione del diritto d'autore

Al fine di dare concreta attuazione organizzativa alle regole generali di prevenzione di cui al precedente paragrafo, di seguito vengono dettagliati i principi di riferimento, diretti a regolamentare la formazione e l'attuazione delle decisioni aziendali, nello svolgimento delle fattispecie di attività sensibili sopra individuate. I medesimi principi vincolano l'operato dei responsabili aziendali anche in assenza di procedure specifiche.

6.1 Gestione della sicurezza fisica e logica dei sistemi informativi

Tale fattispecie di attività sensibile include ogni modalità di forzatura od elusione al livello di sicurezza informatica implementato in Azienda, comprensivo dell'insieme delle misure tecniche e organizzative volte ad assicurare la protezione dell'integrità, della disponibilità, della confidenzialità dell'informazione archiviata in modalità elettronica e delle risorse usate per acquisire, memorizzare, elaborare e comunicare tale informazione.

Il sistema di controllo a presidio delle fattispecie di attività sensibili sopra rilevate, è riepilogato nella seguente tabella.

PRESIDI DI CONTROLLO SPECIFICI E/O LINEE GUIDA PER LA GESTIONE DELLA SICUREZZA FISICA E LOGICA DEI SISTEMI INFORMATIVI
• **Sia previsto un procedimento di autenticazione mediante username e password individuali al quale corrisponda un profilo limitato della gestione di risorse di sistema, specifico per ogni destinatario o categoria di destinatari, le cui password abbiano una scadenza periodica;**

• **Gli utenti di sistemi informatici aziendali siano informati dell'importanza di mantenere le proprie credenziali di accesso al sistema (username e password) confidenziali e di non divulgare le stesse a soggetti terzi;**
• **Gli utenti di sistemi informatici aziendali siano informati della necessità di non lasciare incustodita la propria work-station e della convenienza di bloccarla, qualora si dovessero allontanare dalla postazione di lavoro, con le proprie credenziali di accesso;**
• **I sistemi informatici stessi siano impostati in modo tale che, qualora non vengano utilizzati per un determinato periodo di tempo, si blocchino automaticamente;**
• **I locali in cui è allocato il server centralizzato devono essere chiusi e non accessibili liberamente.**
• **Ogni sistema informatico sia fornito di adeguato software firewall e antivirus e far sì che, ove possibile, questi non possano venir disattivati ai singoli utenti;**
• **Sia testata e monitorata la corretta implementazione delle misure di sicurezza previste dal d.lgs. 196/2003, come aggiornato anche alla luce del Reg. UE 679/2016;**
• **Siano impiegati, sulle apparecchiature della Società, solo prodotti ufficialmente acquistati da Berna Engineering S.r.l.;**
• **Ci si astenga dall'effettuare copie non specificamente autorizzate di dati e di software;**
• **L'accesso a detti locali deve essere consentito solo a soggetti autorizzati (IT) ed attraverso sistema di tracciamento delle visite tramite badge.**

6.2 Gestione e protezione delle reti informatiche aziendali

Tale fattispecie di attività sensibile attiene alla corretta gestione e monitoraggio degli accessi aziendali verso la rete internet e la rete LAN (Local Area Network) aziendale.

Il sistema di controllo a presidio delle fattispecie di attività sensibili sopra rilevate, è riepilogato nella seguente tabella.

PRESIDI DI CONTROLLO SPECIFICI E/O LINEE GUIDA PER GESTIONE E PROTEZIONE DELLE RETI INFORMATICHE AZIENDALI
• **Sia garantito che gli accessi telematici da e verso l'esterno (connessione alla rete Internet) siano autorizzati ed effettuati solo con le modalità consentite dalle procedure aziendali vigenti ed ai fini di utilizzo per scopi lavorativi;**
• **Sia escluso l'accesso ad aree del web e/o a siti Internet particolarmente sensibili poiché veicolo per la distribuzione e diffusione di programmi infetti (c.d. "virus") capaci di danneggiare o distruggere sistemi informatici o dati in questi contenuti (ad esempio, particolari siti di posta elettronica o siti di diffusione di informazioni e files);**
• **La rete LAN aziendale ed ogni sistema informatico societario siano protette, al fine di prevenire l'illecita installazione di dispositivi hardware in grado di intercettare le comunicazioni relative ad un sistema informatico o telematico, o intercorrenti tra più sistemi, ovvero capace di impedirle o interromperle;**
• **Qualora per la connessione alla rete internet si utilizzino collegamenti wireless (ossia senza fili, mediante routers dotati di antenna WiFi), gli stessi vengano protetti impostando una chiave d'accesso, onde impedire che soggetti terzi, esterni alla Società, possano illecitamente collegarsi alla rete Internet tramite i routers della stessa e**

compiere illeciti ascrivibili ai dipendenti della Società, prevedendo eventuale rete dedicata per gli ospiti che non potranno comunque accedere alla rete aziendale;
• **Siano vietati l'installazione e l'utilizzo, sui sistemi informatici della Società, di software (c.d. "P2P", di files sharing o di istant messaging) mediante i quali è possibile scambiare con altri soggetti all'interno della rete Internet ogni tipologia di files (quali filmati, documenti, file audio, virus, etc.) senza alcuna possibilità di controllo da parte della Società;**
• **Sia curata e monitorata l'implementazione delle prescrizioni in materia di amministratori di sistemi informatici introdotte con provvedimento del Garante per la protezione dei dati personali, ai fini di garanzia dell'integrità dei tracciati "log".**

6.3 Gestione e sviluppo di programmi applicativi di proprietà di terzi

Tale fattispecie di attività sensibile include le operazioni di acquisto, distribuzione e manutenzione di programmi applicativi di proprietà di terzi licenziatari, da parte di personale di Berna Engineering S.r.l. Tali attività potrebbero sfociare in fattispecie di abusiva duplicazione di software proprietario non autorizzata dal titolare della licenza di distribuzione, con evidente vantaggio aziendale rappresentato dal risparmio di spesa conseguente al mancato pagamento dei costi di utilizzazione del software.

Il sistema di controllo a presidio delle fattispecie di attività sensibili sopra rilevate, è riepilogato nella seguente tabella.

PRESIDI DI CONTROLLO SPECIFICI E/O LINEE GUIDA PER GESTIONE E SVILUPPO DI PROGRAMMI APPLICATIVI IN PROPRIETÀ DI TERZI
• **Venga redatto, mantenuto ed aggiornato l'inventario dell'hardware e del software in uso agli utenti;**
• **Siano vietati l'installazione e l'utilizzo di software (programmi applicativi) non approvati dalla Società e non correlati con l'attività professionale espletata da parte degli utenti;**
• **Sia vietato l'impiego/uso/installazione sugli strumenti informatici concessi in dotazione dalla Società di materiale copiato/non contrassegnato/non autorizzato;**
• **Siano utilizzati disclaimer su presentazioni, documentazione tecnica, commerciale ecc. che individuino chiaramente il titolare del copyright e la data di creazione;**
• **Siano previste, nei rapporti contrattuali con partner/terzi, clausole di manleva volte a tenere indenne Berna Engineering S.r.l. da eventuali responsabilità in caso di condotte, poste in essere dagli stessi, che possano determinare violazione di qualsiasi diritto di proprietà intellettuale di terze parti.**

6.4 Gestione degli output di sistema e dei dispositivi di memorizzazione

La fattispecie di attività sensibile in esame attiene alla gestione dei supporti magnetici riutilizzabili (penne USB, CD- Rom, *hard-disk* esterni di memorizzazione, ecc.).

Il sistema di controllo a presidio delle fattispecie di attività sensibili sopra rilevate, è riepilogato nella seguente tabella.

PRESIDI DI CONTROLLO SPECIFICI E/O LINEE GUIDA PER GESTIONE DELLA RETE AZIENDALE
• **Siano vietati l'installazione e l'utilizzo su work-station aziendali di supporti magnetici riutilizzabili non forniti direttamente dalla Società e non correlati con l'attività professionale espletata da parte degli utenti o dei consulenti aziendali;**
• **Sia vietato il download di software non autorizzato dalla società, a mezzo di supporti magnetici riutilizzabili;**
• **I supporti magnetici contenenti i dati di back-up siano custoditi in archivi chiusi a chiave e resi accessibili solo agli utenti che necessitano effettivamente di avere disponibilità dei dati recuperati;**
• **Sia definito un sistema di emergenza, comprensivo di tutte le procedure tecnico/organizzative per poter affrontare stati di emergenza e garantire la business continuity attraverso meccanismi di superamento di situazioni anomale (c.d. Disaster Recovery Plan).**

7. Controlli dell'Organismo di Vigilanza

Fatta salva l'attuazione degli ordinari compiti dell'OdV previsti nella Parte Generale del presente Modello, al fine specifico della prevenzione dei reati informatici e dei reati in materia di violazione del diritto d'autore, i controlli dell'OdV investono i seguenti aspetti:

CONTROLLI DELL'ORGANISMO DI VIGILANZA
• **Monitoraggio sull'efficacia e sul rispetto delle regole generali di prevenzione e dei principi di riferimento/protocolli posti a presidio delle fattispecie di attività sensibili;**
• **audit periodici sulla tenuta del sistema di sicurezza informatica aziendale eventualmente con il supporto di outsourcer specializzati;**
• **Verifica a campione sulla conformità dell'operato aziendale alle procedure aziendali adottate nell'ambito della Partizione S.IT, sistemi informativi;**
• **Verifica a campione sulla conformità dell'operato aziendale alle licenze d'uso dei software utilizzati nell'ambito di Berna Engineering S.r.l.;**
• **Esame di eventuali segnalazioni specifiche provenienti dagli altri organi di controllo o da qualsiasi dipendente, in merito alla violazione delle regole generali di prevenzione e dei principi di riferimento a presidio delle suesposte fattispecie di attività sensibili;**
• **Predisposizione degli accertamenti ritenuti necessari od opportuni in conseguenza delle segnalazioni ricevute.**

Nel caso in cui, in seguito agli accertamenti svolti dall'OdV, emergessero elementi che facciano risalire alla scoperta della commissione di uno dei reati contemplati nella presente Sezione della Parte Speciale, o al tentativo di commissione di uno dei reati suddetti, l'OdV dovrà riferire all'Amministratore Unico di Berna Engineering S.r.l., al quale compete ogni decisione in merito alle sanzioni irrogabili.