RPG S.R.L.

Parte Speciale - Sezione B: reati informatici e diritto d’autore

Documento integrante il Modello di organizzazione, gestione e controllo ai sensi del d.lgs. 8 giugno 2001, n. 231

Adottato con delibera dell’Amministratore Unico in data 21/09/2026

Edizione 2026 - aggiornamento normativo al 2 agosto 2026

ID documento	Versione	Contenuto	Approvazione	Controllo
MOG231_RPG_PARTE SPECIALE_SEZ.B	VER.1.1_2026	Revisione integrativa DVR/POS, organico e autonomia societaria 2026	Amministratore Unico	Organismo di Vigilanza

Sommario

- 1. Scopo
- 2. Principi
- 3. Reati
- 4. Attività sensibili
- 5. Protocolli
- 6. Flussi OdV

1. Scopo e campo di applicazione

La Sezione presidia l'uso di piattaforme di gara, posta elettronica certificata, firme digitali, software gestionali, dispositivi di cantiere, archivi tecnici e dati personali.

La Sezione presidia i reati richiamati dagli artt. 24-bis e 25-novies del d.lgs. 231/2001, nei limiti della loro astratta applicabilità alla Società. Il richiamo alle fattispecie è funzionale alla prevenzione e non sostituisce il testo di legge vigente.

2. Principi generali

- Legalità e tracciabilità delle decisioni.
- Separazione tra attività operative, autorizzative e di controllo.
- Veridicità dei dati e dei documenti.
- Divieto di ricorso a terzi per eludere i protocolli.
- Obbligo di segnalare anomalie, conflitti, pressioni e violazioni.
- Conservazione delle evidenze e disponibilità per l'OdV.

3. Reati rilevanti

- Accesso abusivo, intercettazione illecita e danneggiamento di dati o sistemi.
- Detenzione o diffusione abusiva di credenziali e strumenti informatici.
- Falsità in documenti informatici.
- Estorsione mediante reati informatici.
- Duplicazione o uso illecito di software, banche dati e opere protette.

Protocolli di controllo

Attività sensibile	Rischio/modalità	Controlli obbligatori	Evidenze
Credenziali e firme	Uso da parte di terzi o operazioni non autorizzate	Assegnazione nominativa; MFA ove disponibile; divieto condivisione; revoca immediata; registro dispositivi	Elenco utenze; log; verbali consegna/revoca
Piattaforme di gara	Alterazione documenti, invio non autorizzato, perdita scadenze	Profilazione; doppia verifica file; ricevute; backup; calendario scadenze	Ricevute; hash/versioni; check-list invio
PEC e documenti	Cancellazione, spoofing, invio a destinatari errati	Accessi limitati; archiviazione; regole di inoltro; verifica destinatari e allegati	Registro PEC; esportazioni; audit log
Software	Licenze illecite o installazioni rischiose	Inventario; acquisti autorizzati; divieto software personale; aggiornamenti	Licenze; inventario; ticket
Dati e backup	Perdita, cifratura, esfiltrazione	Backup periodici; test ripristino; antivirus/EDR; patching; segregazione	Report backup; test; alert
Incidenti	Ritardo nella risposta o occultamento	Procedura incident response; isolamento; conservazione log; valutazione data breach; flusso OdV	Scheda incidente; cronologia; azioni
Fornitori IT	Accessi permanenti o incontrollati	Contratto; autorizzazione accessi; logging; riservatezza; revoca	Contratto; elenco accessi; report

6. Flussi OdV

- Incidenti informatici, ransomware, accessi abusivi e data breach.
- Creazione o revoca di utenze privilegiate.
- Anomalie nelle piattaforme di gara o nelle firme digitali.
- Software non autorizzato o contestazioni su licenze.
- Esiti dei test di backup e principali vulnerabilità.