Modello di Organizzazione e Gestione (MOG 231) e Piano di Prevenzione della Corruzione e della Trasparenza (PTPCT)

Ai sensi del Decreto Legislativo 8 giugno 2001, n. 231 e della Legge 6 novembre 2012, n. 190, recante "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione" e s.m.i.

Parte Speciale – Allegato L
Protocollo di Controllo
Gestione dei sistemi informativi e sicurezza dati

SCHEDA CONTROLLO DOCUMENTO

IDENTIFICAZIONE

TITOLO DEL DOCUMENTO	Modello di Organizzazione e gestione ai sensi del Decreto legislativo 8 giugno 2001, n. 231 *Parte Speciale – Allegato L* *Protocollo di controllo – Gestione dei sistemi informativi e sicurezza dati*

Controllo del documento storico

TITOLO	VERSIONE	DATA EMISSIONE	COMMENTO	FIRMA
"Criminalità Informatica, violazione del diritto d'autore"	00	23.02.2011	Prima emissione	
Protocollo di controllo "Gestione dei sistemin informative e Sicurezza dati"	1.0	18/06/2014	Prima emissione	
Protocollo di controllo "Gestione dei sistemin informative e Sicurezza dati"	Rev. 01		Rev. 01 dell'emissione del 18.06.2014	

Aggiornamento normativo del 13.12.2019 a cura del Servizio Supporto Attività Istituzionali e Progetto 231-RPCT con la collaborazione del Dott. Umberto Poli nell'ambito dell'incarico autorizzato con riferimento prot. n. 4000 del 9 aprile 2018.

Approvato con delibera del CdA n. 12 del 29.01.2020

Indice

1. Definizioni

- **CdA**: Consiglio di Amministrazione di Romagna Acque - Società delle Fonti S.p.A.
- **Decreto 231**: Decreto Legislativo 8 giugno 2001, n. 231
- **Decreto Privacy:** Decreto Legislativo 30 giugno 2003, n. 196
- **Modello 231:** Modello di organizzazione e gestione *ex* articolo 6 del Decreto Legislativo 8 giugno 2001, n. 231
- **Legge 190/2012 o Legge Anticorruzione:** Legge del 6 novembre 2012 n.190 "Disposizione per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione", e relativi provvedimenti ampliativi
- **OdV**: Organismo di Vigilanza ex articolo 6 del Decreto Legislativo 8 giugno 2001, n. 231
- **Romagna Acque o Società:** Romagna Acque - Società delle Fonti S.p.A.

2. Reati

Il presente paragrafo illustra brevemente il "reato di corruzione tra privati, i "reati societari", i "reati informatici" ed i "delitti in materia di violazione del diritto d'autore", previsti dal D.lgs. n. 231/2001 all'art. 24 *bis*, all'art. 25 *ter* e all'art. 25 *novies*, in modo da acquisire nozioni utili alla comprensione ed attuazione del presente protocollo.
Per l'analisi completa dei reati si rimanda allo "Schema riepilogativo reati", documento allegato al Modello 231.

INDEBITA PERCEZIONE DI EROGAZIONI, TRUFFA IN DANNO DELLO STATO O DI UN ENTE PUBBLICO O PER IL CONSEGUIMENTO DI EROGAZIONI PUBBLICHE E FRODE INFORMATICA IN DANNO DELLO STATO O DI UN ENTE PUBBLICO (Art. 24 del D.lgs. 231/2001)

1. **Frode informatica (art. 640 *ter* c.p.)**

Tale ipotesi di reato si configura nel caso in cui, alterando il funzionamento di un sistema informatico o telematico o manipolando i dati in esso contenuti, si ottenga un ingiusto profitto arrecando danni allo Stato o ad altro ente pubblico.
L'alterazione fraudolenta del sistema può essere la conseguenza di un intervento rivolto sia alla componente meccanica dell'elaboratore, sia al software.
Sono considerate pertinenti ad un sistema informatico e quindi rilevanti ai sensi della normativa in questione le informazioni contenute su supporti materiali, nonché i dati e i programmi contenuti su supporti esterni all'elaboratore (come dischi, nastri magnetici e ottici) che siano destinati ad essere utilizzati in un sistema informatico.
In concreto può integrarsi il reato in esame, qualora, una volta ottenuto un finanziamento, venisse violato il sistema informatico al fine di inserire un importo relativo ai finanziamenti superiore a quelle ottenuto legittimamente ovvero nel caso in cui si alteri il funzionamento di un sistema informatico o dei dati in esso contenuti al fine di modificare le risultanze relative al versamento dei contributi previdenziali.

DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI (Art. 24 *bis* del D.lgs. 231/2001)

2. Documenti informatici (art. 491 *bis* c.p.)

Tale tipologia di reato punisce chi integra uno dei reati relativi alle falsità in atti, se alcuna delle falsità previste dal Libro II, Titolo VII, Capo III Codice Penale, riguarda un documento informatico pubblico o privato, avente efficacia probatoria.

Di seguito si riportano alcune delle tipologie delittuose particolarmente rilevanti, a titolo esemplificativo:

- falsità materiali commesse da un pubblico ufficiale o da un incaricato di pubblico servizio in atti pubblici e documenti ad essi assimilabili;
- falsità materiali in scrittura privata;
- falsità ideologiche in documenti pubblici commesse da un pubblico ufficiale, da un incaricato di pubblico servizio ovvero da un privato;
- uso di atto falso (qualora l'autore materiale non sia precedentemente concorso nella falsificazione del documento);
- soppressione, distruzione e occultamento, parziale o totale, di atti veri.

3. Accesso abusivo ad un sistema informatico o telematico (art. 615 *ter* c.p.)

Tale tipologia di reato si configura nel caso in cui un soggetto, abusivamente, si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

4. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 *quater* c.p.)

Tale reato si configura nel caso in cui un soggetto, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo.

5. Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 *quinquies* c.p.)

Il reato in oggetto si configura nel caso in cui un soggetto, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri, apparecchiature, dispositivi o programmi informatici.

6. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 *quater* c.p.)

Il reato si realizza nel momento in cui un soggetto, fraudolentemente, intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe. Allo stesso modo compie un reato chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al paragrafo precedente.

7. Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 *quinquies* c.p.)

Il reato in oggetto si configura nel caso in cui un soggetto, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi.

8. Danneggiamento di informazioni, dati e programmi informatici (art. 635 *bis* c.p.)

Il reato in oggetto si configura nel caso in cui un soggetto, salvo che il fatto costituisca più grave reato, distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui.

9. 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.)

Il reato in oggetto si configura nel caso in cui un soggetto commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità.

10. Danneggiamento di sistemi informatici o telematici (art. 635 *quater* c.p.)

Il reato in oggetto si configura nel caso in cui un soggetto, mediante le condotte di cui all'articolo 635-*bis*, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento.

11. Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 *quinquies* c.p.)

La norma prevede sanzioni nel caso in cui il fatto previsto dal precedente art. 635 *quater* è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.

DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE (Art. 25 *novies* del D.lgs. 231/2001):

12.

- **Art. 171, primo comma, lettera a-*bis*, L. 633/1941**

La norma punisce chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa. Il reato è più grave se commesso sopra un'opera altrui non destinata alla pubblicazione, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore.

- **Art. 171, terzo comma, L. 633/1941**

La norma prevede per i reati di cui al primo comma, lettere da *a)* ad *f)* della stessa Legge sanzioni aggravate qualora siano "commessi sopra un'opera altrui non destinata alla pubblicazione, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore o alla reputazione dell'autore.

- **Art. 171 *bis*, L. 633/1941**

La norma punisce la condotta di chi abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE); utilizza qualsiasi mezzo inteso a consentire o facilitare la rimozione arbitraria o l'elusione di protezioni di un software; al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati, esegue l'estrazione o il reimpiego della banca di dati, distribuisce, vende o concede in locazione una banca di dati.

- **Art. 171 *ter*, L. 633/1941**

Punisce chi – tra l'altro – abusivamente duplica, riproduce, trasmette o diffonde in pubblico opere dell'ingegno destinate al circuito televisivo, cinematografico, opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico - musicali e multimediali.

- **Art. 171 *septies*, L. 633/1941**

Punisce la mancata comunicazione o falsa dichiarazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno.

- **Art. 171 *octies*, L. 633/1941**

La norma punisce chiunque a fini fraudolenti produce, pone in vendita, importa, promuove, installa, modifica, utilizza per uso pubblico e privato apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale.

3. Area a rischio n. 1: "Gestione dei sistemi informativi aziendali"

3.1. Funzioni aziendali coinvolte

Le funzioni aziendali della Società coinvolte nell'attività di gestione dei sistemi informativi aziendali sono rappresentate dalle seguenti:
- Direttore generale;
- Area Servizi – Servizi Sistemi informativi e Telecomunicazioni;
- Area Amministrazione, Finanza, Pianificazione e Controllo, Personale e Organizzazione;
- Dipendenti di Romagna Acque assegnatari di strumenti hardware e software aziendali.

3.2. Attività sensibili

Nell'ambito della sopra indicata area a rischio n. 1 si individuano le specifiche attività sensibili di seguito elencate:
- Gestione dei sistemi informatici;
- Gestione degli accessi logici ai dati e ai sistemi;
- Gestione del software, apparecchiature, dispositivi o programmi informatici;
- Gestione della rete e dell'hardware;
- Gestione della sicurezza fisica;
- Gestione outsourcing IT;
- Utilizzo della postazione di lavoro;
- Installazione, manutenzione, aggiornamento e gestione di software di soggetti pubblici o forniti da terzi per conto di soggetti pubblici;
- Gestione di reti di fibra ottica spenta
- Gestione del backup.

3.3. Reati astrattamente ipotizzabili

Si elencano di seguito i possibili reati configurabili con riferimento alle attività sensibili individuate nella presente area a rischio:
1. Frode informatica (art. 640 *ter* c.p.)
2. Documenti informatici (art. 491 *bis* c.p.)
3. Accesso abusivo ad un sistema informatico o telematico (art. 615 *ter* c.p.)
4. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 *quater* c.p.)
5. Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 *quinquies* c.p.)
6. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 *quater* c.p.)
7. Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617 *quinquies* c.p.)
8. Danneggiamento di informazioni, dati e programmi informatici (art. 635 *bis* c.p.)
9. 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.)
10. Danneggiamento di sistemi informatici o telematici (art. 635 *quater* c.p.)

11. Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 *quinquies* c.p.)
12. Art. 171 *bis* L. 633/1941 comma 1 - Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori.

3.4. Esempi di possibili modalità di realizzazione del reato e relative finalità

Per ciascuna categoria di delitti in materia informatica, si evidenziano alcuni esempi di modalità di commissione.

Con riferimento al reato di indebita percezione di erogazioni, truffa in danno dello stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico (ai sensi dell'art. 24 del D.lgs. 231/2001), si potrebbe configurare la seguente modalità di realizzazione del reato:

1. Alterazione del funzionamento di un sistema informatico o telematico o di intervento senza diritto su dati, informazioni, programmi allo scopo di trarne profitto con danno d'altri. A titolo meramente esemplificativo e non esaustivo, il reato è configurabile qualora, attraverso l'alterazione del software di controllo INPS per le denunce retributive, si ottenga un ingiusto vantaggio con danno dell'ente previdenziale.

Con riferimento ai delitti informatici e trattamento illecito di dati (ai sensi dell'art. 24 *bis* del D.lgs. 231/2001), si potrebbero configurare le seguenti modalità di realizzazioni di reati:

2. Il reato previsto dall'art. 491 *bis* c.p. potrebbe configurarsi qualora, nell'interesse o a vantaggio della Società, un dipendente di Romagna Acque dovesse effettuare un accesso non autorizzato al fine di modificare un documento informatico;

4. Il reato previsto dall'art. 615 *quater* c.p. si potrebbe configurare a titolo meramente esemplificativo, qualora un dipendente della Società, nell'interesse o a vantaggio della medesima, diffondesse abusivamente codici di accesso a sistemi informativi della Società o di terze parti verso un fornitore di servizi informativi per trarne un profitto o arrecare ad altri un danno;

5. Il reato previsto dall'art. 615 *quinquies* c.p. si potrebbe configurare qualora, nell'interesse o a vantaggio della Società, un dipendente di Romagna Acque diffondesse codice malevolo al fine di danneggiare i sistemi informatici o siti web di aziende concorrenti e conseguentemente incrementare la quota di mercato della Società;

6. Il reato previsto dall'art. 617 *quater* si potrebbe configurare, a titolo meramente esemplificativo, qualora un dipendente della Società, nell'interesse o a vantaggio della Società, intercettasse comunicazioni o informazioni di terze parti che potrebbero assumere rilevanza con riferimento ad operazioni straordinarie;

7. Il reato previsto dall'art. 617 *quinquies* c.p. si potrebbe configurare, a titolo meramente esemplificativo, qualora un dipendente della Società, nell'interesse o a vantaggio della Società, installasse abusivamente apparecchiature finalizzate all'intercettazione di comunicazioni o informazioni di terze parti che potrebbero assumere rilevanza con riferimento ad operazioni straordinarie;

8. Il reato previsto dall'art. 635 *bis* c.p. si potrebbe configurare, a titolo meramente esemplificativo, qualora un dipendente della Società, nell'interesse o a vantaggio della medesima, danneggia i programmi informatici di terze parti;

9. Il reato previsto dall'art. 635 *ter* c.p. si potrebbe configurare, a titolo meramente esemplificativo, qualora un dipendente della Società, nell'interesse o a vantaggio della medesima, danneggia i programmi informatici di pubblica utilità;

10. Il reato previsto dall'art, 635 *quater* c.p. si potrebbe configurare, a titolo meramente esemplificativo, qualora un dipendente della Società, nell'interesse o a vantaggio della medesima, danneggia sistemi informatici o telematici.

Il reato di criminalità informatica potrebbe configurarsi nell'interesse o a vantaggio della Società mediante i seguenti comportamenti illeciti:

3. Accedere abusivamente (senza autorizzazione) ad un sistema informatico protetto;

4. Ottenere, riprodurre, diffondere, comunicare o divulgare codici di accesso a sistemi informatici protetti o crittati;

7.

- 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);

8. Diffondere programmi capaci di infettare un sistema per manometterne la regolare funzionalità (ad es. il sistema informatico di un competitor);

10. Falsare un documento informatico, ovvero un supporto informatico contenente dati od informazioni avente efficacia probatoria oppure un programma specificamente destinato ad elaborarlo.

Con riferimento ai reati commessi in violazione del diritto d'autore, la Società potrebbe invece, ad esempio:

12.

- Utilizzare illecitamente software protetto da diritto d'autore senza averne in tutto o in parte acquistate le dovute licenze, permettendo così di conseguire un ingiusto vantaggio economico equivalente al mancato sostenimento dei costi necessari per il regolare acquisto dei programmi;
- Duplicare abusivamente programmi coperti da licenza al fine di trarne vantaggi in termini di risparmio di costi.

3.5. Controlli chiave necessari a fronte dei rischi rilevati

Obiettivo del presente protocollo è garantire che tutti i soggetti, a vario titolo coinvolti nei processi sopra elencati, mantengano condotte conformi alla politica aziendale tali da impedire e prevenire la commissione dei reati indicati nei precedenti paragrafi.
La Società ha predisposto e implementato appositi presidi organizzativi atti a prevenire e controllare il rischio di commissione di reato nello svolgimento delle proprie attività. Tutte le funzioni coinvolte in tali

attività sono tenute ad osservare le disposizioni di legge esistenti in materia, la normativa interna, nonché quanto previsto dal Codice Etico e dalle procedure aziendali.
Di seguito sono riportati i controlli chiave necessari a fronte dei rischi rilevati nei processi sopra elencati:

- Attribuire ai soggetti aziendali l'obbligo di trasmettere flussi informativi periodici all'OdV, allo scopo di garantire un corretto monitoraggio sulle attività sensibili;
- Svolgere controlli specifici nelle seguenti aree:
  - Utilizzo della postazione di lavoro;
  - Gestione dei sistemi software;
  - Installazione, manutenzione, aggiornamento e gestione di software di soggetti pubblici o forniti da terzi per conto di soggetti pubblici;
  - Gestione degli accessi logici;
  - Gestione della rete e dell'hardware;
  - Gestione della sicurezza fisica;
  - Gestione dei servizi di outsourcing IT;
  - Gestione di reti di fibra ottica spenta.
- Prevedere che i codici identificativi (*user-id*) per l'accesso alle applicazioni ed alla rete siano individuali ed univoci;
- Prevedere specifici criteri per l'assegnazione e la creazione, modifica e aggiornamento delle password di accesso alla rete, alle applicazioni, al patrimonio informativo aziendale e ai sistemi critici o sensibili (ad es. lunghezza minima della password, regole di complessità, scadenza periodica);
- Garantire una corretta regolamentazione per l'assegnazione delle utenze e dei ruoli, compresi i ruoli applicativi con privilegi speciali (*super user*) e l'esplicitazione del *workflow* operativo, degli step autorizzativi necessari nonché delle responsabilità connesse alla revisione periodica dei profili assegnati con i responsabili aziendali;
- Garantire l'individuazione dei database contenenti informazioni critiche e la protezione dei dati con l'utilizzo di strumenti crittografici;
- Formalizzare procedure/protocolli di controllo per la generazione e la protezione dei *log* delle attività sui sistemi;
- Prevedere, nell'ambito della creazione e della assegnazione dei profili autorizzativi ai dipendenti, che la password di rete inizialmente creata di default dagli Amministratori di Sistema e assegnata ai dipendenti, sia conservata correttamente e cambiata periodicamente;
- Prevedere il divieto assoluto di cedere e/o comunicare a terzi la password;
- Garantire che l'accesso agli applicativi gestionali ed informativi finalizzato alla modifica dati, ovvero a qualsivoglia intervento sui programmi destinati ad elaborarli, deve avvenire in modo tale che l'utente sia autorizzato ad accedervi limitatamente alla fase di sua competenza;
- Garantire che le applicazioni tengano traccia dell'effettuazione di operazioni e delle modifiche ai dati compiute dagli utenti;
- Definire i criteri e le modalità per l'assegnazione, la modifica e la cancellazione dei profili utente;
- Formalizzare i criteri e le modalità per la gestione di: *(i)* nuovi utenti (al momento di assunzione del dipendente) e *(ii)* cambio di responsabilità (in caso di regresso);
- Eseguire verifiche periodiche dei profili utente al fine di verificare che siano coerenti con le responsabilità assegnate e coerente con i principi di segregazione dei ruoli;
- Classificare tutti i dati, e non solo quelli rilevanti ai sensi del Codice della Privacy, in funzione dei requisiti di sicurezza (riservatezza, disponibilità, integrità);
- Garantire l'acquisto e l'uso esclusivamente di software autorizzato e certificato;
- Garantire che per installare software diversi da quelli messi a disposizione dalla Società, sia necessario richiedere autorizzazione preventiva all'Amministratore di Sistema;

- Compilare e mantenere aggiornato un inventario dell'hardware e del software in uso presso la Società;
- Formalizzare i criteri e le modalità per il processo di *change management* (inteso come aggiornamento o implementazione di nuovi sistemi/servizi tecnologici), che definisca, oltre alle responsabilità e alle principali fasi del processo di sviluppo, l'attività di formalizzazione dei test e le modalità di approvazione delle modifiche software effettuate prima del rilascio in ambiente di produzione;
- Istituire e mantenere aggiornato un inventario del software in uso dagli utenti;
- Prevedere specifiche attività di controllo periodico dello sviluppo di software all'interno della Società e di quello affidato in outsourcing;
- Pianificare verifiche periodiche sull'utilizzo di internet al fine di evidenziare comportamenti anomali, garantendo il trattamento dei dati in forma anonima o tale da precludere l'immediata identificazione degli utenti mediante opportune aggregazioni;
- Garantire una revisione periodica degli accessi e delle attività svolte dai fornitori di servizi informatici;
- Assegnare formalmente gli accessi remoti ai sistemi effettuati da terzi;
- Prevedere un piano di *business continuity* ed uno di *disaster recovery* periodicamente aggiornati e testati;
- Far compilare e far accettare formalmente a tutti gli assegnatari della dotazione informatica hardware e software una "scheda di presa in carico" dove, previa elencazione di tutta la strumentazione hardware e software fornita, vengono descritte le condizioni d'uso che tutto il personale si impegna a rispettare;
- Prevedere, nella suesposta "scheda di presa in carico":
  - l'obbligo di utilizzare il PC per le sole esigenze di servizio;
  - l'obbligo di non cedere, in nessun caso, neppure in via temporanea, l'uso del PC a terzi, né a titolo gratuito né a titolo oneroso, tenendo, in particolare, segreta la password per il collegamento da remoto alla rete aziendale, laddove previsto;
  - il divieto di istallare software non forniti da Romagna Acque, ancorché distribuiti gratuitamente, salvo preventiva autorizzazione dell'Amministratore di Sistema;
  - l'obbligo di conservare e custodire con cura e con la massima diligenza il PC provvedendo alla restituzione dello stesso nello stato attuale, salvo il normale deterioramento, non appena richiesto dalla Società e comunque non oltre il termine massimo da quest'ultima eventualmente fissato, senza possibilità di opporre eccezione alcuna;
  - l'obbligo di comunicare con la massima tempestività l'eventuale smarrimento e/o furto del PC informando in ogni caso la società circa la natura e l'entità dei dati aziendali in esso memorizzati;
  - l'obbligo di comunicare gli eventuali malfunzionamenti del PC alla Società mettendo in qualsiasi momento il PC stesso a disposizione della Società o di un suo incaricato per ogni operazione di manutenzione e/o riparazione che dovesse essere ritenuta necessaria;
- Gestire la fase della riconsegna del materiale attraverso la compilazione della scheda "Restituzione della dotazione informatica", dove viene fatto espresso divieto di criptare, riservare, rendere comunque inutilizzabili i dati contenuti nel PC oggetto di riconsegna;
- Archiviare la documentazione riguardante ogni singola attività allo scopo di garantire la completa tracciabilità della stessa;
- Definire i criteri e le modalità per la gestione dei sistemi hardware che prevedano la compilazione e la manutenzione di un inventario aggiornato dell'hardware in uso presso la Società e che regolamentino le responsabilità e le modalità operative in caso di implementazione e/o manutenzione di hardware;
- Definire i criteri e le modalità per le attività di *back up* che prevedano, per ogni applicazione hardware, la frequenza dell'attività, le modalità, il numero di copie ed il periodo di conservazione dei dati;

- Definire i criteri e le modalità per la gestione dei sistemi software che prevedano la compilazione e manutenzione di un inventario aggiornato del software in uso presso la società, l'utilizzo di software formalmente autorizzato e certificato e l'effettuazione di verifiche periodiche sui software installati e sulle memorie di massa dei sistemi in uso al fine di controllare la presenza di software proibiti e/o potenzialmente nocivi;
- Definire le credenziali fisiche di accesso ai siti ove risiedono i sistemi informativi e le infrastrutture IT quali, a titolo esemplificativo, badge e chiavi;
- Prevedere ruoli e responsabilità dei soggetti che usano i sistemi informatici e le piattaforme telematiche gestiti da terzi, ivi inclusi ruoli e responsabilità di coloro che operano attraverso strumentazione informatica e telematica;
- Adottare sistemi idonei alla registrazione degli accessi mediante autenticazione informatica ai sistemi informatici e agli archivi elettronici da parte di tutti i dipendenti ivi inclusi gli Amministratori di Sistema;
- Prevedere limitazioni alla possibilità di scaricare materiale dalla rete internet, adottando sistemi informatici idonei a limitare la possibilità di effettuare download e/o operazioni analoghe non autorizzate;
- Impostare le postazioni di lavoro in modo tale che, qualora non vengano utilizzati per un determinato periodo di tempo, si blocchino automaticamente;
- Dotare tutti i sistemi informatici di adeguato software *firewall* e *antivirus* e far sì che, ove possibile, questi non possano venir disattivati;
- Implementare dei controlli di sicurezza per garantire la riservatezza dei dati all'interno della rete e di quelli in transito su reti pubbliche;
- Adottare strumenti e soluzioni di monitoraggio del traffico di rete;
- Garantire una sicura gestione degli incidenti di sicurezza;
- Garantire lo smaltimento ed il riutilizzo sicuro delle attrezzature e dei supporti;
- Garantire la identificazione delle responsabilità per l'autorizzazione degli accessi fisici, il *workflow* per la concessione di tali permessi e gli step autorizzativi;
- Limitare gli accessi alle stanze server unicamente al personale autorizzato;
- Migliorare il processo di inventariazione dei beni e strumenti informatici allo scopo di tracciare e monitorare apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche;
- Informare gli utilizzatori dei sistemi informatici che i software per l'esercizio delle attività di loro competenza sono protetti dalle leggi sul diritto d'autore ed in quanto tali ne è vietata la duplicazione, la distribuzione, la vendita o la detenzione a scopo commerciale/imprenditoriale;
- Garantire che i contratti che regolano i rapporti con i fornitori delle presenti attività (servizi in *outsourcing*) prevedano apposite clausole che impongano:
  - la conformità dei software forniti a leggi e normative applicabili;
  - la manleva per la Società in caso di violazioni commesse dai fornitori del servizio stessi.
- Garantire che ai contratti che regolano i rapporti con i fornitori siano apposte clausole che richiamano gli adempimenti e le responsabilità derivanti dal Decreto 231 e dal rispetto dei principi fondamentali del Modello 231 e del Codice Etico e che indicano chiari effetti contrattuali in merito al mancato rispetto di detti adempimenti;
- Implementare meccanismi di tracciatura degli eventi di sicurezza sulle reti (ad es. accessi anomali per frequenza, modalità, temporalità);
- Garantire l'implementazione e la manutenzione delle reti telematiche mediante la definizione di responsabilità e modalità operative, di verifiche periodiche sul funzionamento delle reti e sulle anomalie riscontrate; inoltre, sia regolamentata l'esecuzione di attività periodiche di *vulnerability assessment* ed *ethical hacking*;
- Definire le responsabilità per la gestione delle reti;

- Garantire che nessun dipendente acceda in maniera abusiva ai sistemi informativi utilizzati dalla Pubblica Amministrazione o ne alteri in qualsiasi modo il funzionamento oppure intervenga con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico per ottenere e/o modificare indebitamente informazioni a vantaggio dell'azienda od a terzi;
- Informare adeguatamente i dipendenti della Società e gli altri soggetti eventualmente autorizzati all'utilizzo dei Sistemi Informativi, come ad esempio i collaboratori esterni, dell'importanza di:
  - Mantenere le proprie credenziali confidenziali e di non divulgare le stesse a soggetti terzi;
  - Utilizzare correttamente i software e le banche dati in dotazione;
  - Non utilizzare dati, immagini o altro materiale coperto dal diritto d'autore senza avere ottenuto le necessarie autorizzazioni dai propri superiori gerarchici secondo le indicazioni contenute nelle *policy* aziendali.
- Curare l'informativa diretta agli utilizzatori dei sistemi informatici volta a diffondere la consapevolezza che tutti i software forniti dalla Società sono protetti dalle leggi sul diritto d'autore ed in quanto tali ne è vietata la duplicazione, la distribuzione, la vendita o la detenzione a scopo commerciale/imprenditoriale;
- Nell'ambito della gestione di reti di fibra ottica spenta, ai fini di prevenire fenomeni di tipo corruttivo:
  - Identificare i soggetti che intrattengono rapporti con soggetti privati nell'ambito della gestione di reti di fibra ottica spenta;
  - Garantire la tracciabilità delle informazioni fornite e ricevute a/dai suddetti soggetti privati;
  - Garantire costantemente specifici flussi informativi verso l'OdV e riferimenti puntuali alle sezioni rilevanti del Codice Etico adottato dalla Società;
  - Garantire la corretta archiviazione della documentazione riguardante ogni singola attività prevista dal presente processo allo scopo di garantire la completa tracciabilità dello stesso.

3.6. Sistema autorizzativo e segregazione delle funzioni

La Società, con riferimento all'area a rischio in oggetto, ha assegnato le seguenti responsabilità, rispondendo a criteri di segregazione delle funzioni, al fine di consentire un efficace monitoraggio.

È compito della Funzione "Sistemi Informativi e Telecomunicazioni":

- Prevedere che i codici identificativi (*user-id*) per l'accesso alle applicazioni ed alla rete siano individuali ed univoci;
- Prevedere specifici criteri per l'assegnazione e la creazione, modifica e aggiornamento delle password di accesso alla rete, alle applicazioni, al patrimonio informativo aziendale e ai sistemi critici o sensibili (ad es. lunghezza minima della password, regole di complessità, scadenza periodica);
- Garantire una corretta regolamentazione per l'assegnazione delle utenze e dei ruoli, compresi i ruoli applicativi con privilegi speciali (*super user*) e l'esplicitazione del *workflow* operativo, degli step autorizzativi necessari nonché delle responsabilità connesse alla revisione periodica dei profili assegnati con i responsabili aziendali;
- Garantire l'individuazione dei database contenenti informazioni critiche e la protezione dei dati con l'utilizzo di strumenti crittografici;
- Formalizzare procedure/protocolli di controllo per la generazione e la protezione dei *log* delle attività sui sistemi;
- Prevedere, nell'ambito della creazione e della assegnazione dei profili autorizzativi ai dipendenti, che la password di rete inizialmente creata di default dagli Amministratori di Sistema e assegnata ai dipendenti, sia conservata correttamente e cambiata periodicamente;
- Prevedere il divieto assoluto di cedere e/o comunicare a terzi la *password*;

- Garantire che l'accesso agli applicativi gestionali ed informativi finalizzato alla modifica dati, ovvero a qualsivoglia intervento sui programmi destinati ad elaborarli, deve avvenire in modo tale che l'utente sia autorizzato ad accedervi limitatamente alla fase di sua competenza;
- Garantire che le applicazioni tengano traccia dell'effettuazione di operazioni e delle modifiche ai dati compiute dagli utenti;
- Definire i criteri e le modalità per l'assegnazione, la modifica e la cancellazione dei profili utente;
- Formalizzare criteri e modalità per la gestione di: *(i)* nuovi utenti (al momento di assunzione del dipendente) e *(ii)* cambio di responsabilità (in caso di regresso);
- Eseguire verifiche periodiche dei profili utente al fine di verificare che siano coerenti con le responsabilità assegnate e coerente con i principi di segregazione dei ruoli;
- Classificare tutti i dati, e non solo quelli rilevanti ai sensi del Codice della Privacy, in funzione dei requisiti di sicurezza (riservatezza, disponibilità, integrità);
- Garantire l'acquisto e l'uso esclusivamente di software autorizzato e certificato;
- Garantire che per installare software diversi da quelli messi a disposizione dalla Società, sia necessario richiedere autorizzazione preventiva all'Amministratore di Sistema;
- Compilare e mantenere aggiornato un inventario dell'hardware e del software in uso presso la Società;
- Formalizzare i criteri e le modalità per il processo di *change management* (inteso come aggiornamento o implementazione di nuovi sistemi/servizi tecnologici), che definisca, oltre alle responsabilità e alle principali fasi del processo di sviluppo, l'attività di formalizzazione dei test e le modalità di approvazione delle modifiche software effettuate prima del rilascio in ambiente di produzione;
- Istituire e mantenere aggiornato un inventario del software in uso dagli utenti;
- Prevedere specifiche attività di controllo periodico dello sviluppo di software all'interno della Società e di quello affidato in *outsourcing*;
- Pianificare verifiche periodiche sull'utilizzo di internet al fine di evidenziare comportamenti anomali, garantendo il trattamento dei dati in forma anonima o tale da precludere l'immediata identificazione degli utenti mediante opportune aggregazioni;
- Garantire una revisione periodica degli accessi e delle attività svolte dai fornitori di servizi informatici;
- Assegnare formalmente gli accessi remoti ai sistemi effettuati da terzi;
- Prevedere un piano di *business continuity* ed uno di *disaster recovery* periodicamente aggiornati e testati;
- Archiviare la documentazione riguardante ogni singola attività allo scopo di garantire la completa tracciabilità della stessa;
- Definire i criteri e le modalità per la gestione dei sistemi hardware che prevedano la compilazione e la manutenzione di un inventario aggiornato dell'hardware in uso presso la Società e che regolamentino le responsabilità e le modalità operative in caso di implementazione e/o manutenzione di hardware;
- Definire i criteri e le modalità per le attività di *back up* che prevedano, per ogni applicazione hardware, la frequenza dell'attività, le modalità, il numero di copie ed il periodo di conservazione dei dati;
- Definire i criteri e le modalità per la gestione dei sistemi software che prevedano la compilazione e manutenzione di un inventario aggiornato del software in uso presso la società, l'utilizzo di software formalmente autorizzato e certificato e l'effettuazione di verifiche periodiche sui software installati e sulle memorie di massa dei sistemi in uso al fine di controllare la presenza di software proibiti e/o potenzialmente nocivi;
- Definire le credenziali fisiche di accesso ai siti ove risiedono i sistemi informativi e le infrastrutture IT quali, a titolo esemplificativo, badge e chiavi;

- Prevedere ruoli e responsabilità dei soggetti che usano i sistemi informatici e le piattaforme telematiche gestiti da terzi, ivi inclusi ruoli e responsabilità di coloro che operano attraverso strumentazione informatica e telematica;
- Adottare sistemi idonei alla registrazione degli accessi mediante autenticazione informatica ai sistemi informatici e agli archivi elettronici da parte di tutti i dipendenti ivi inclusi gli Amministratori di Sistema;
- Prevedere limitazioni alla possibilità di scaricare materiale dalla rete internet, adottando sistemi informatici idonei a limitare la possibilità di effettuare download e/o operazioni analoghe non autorizzate;
- Impostare le postazioni di lavoro in modo tale che, qualora non vengano utilizzati per un determinato periodo di tempo, si blocchino automaticamente;
- Dotare tutti i sistemi informatici di adeguato software *firewall* e *antivirus* e far sì che, ove possibile, questi non possano venir disattivati;
- Implementare dei controlli di sicurezza per garantire la riservatezza dei dati all'interno della rete e di quelli in transito su reti pubbliche;
- Adottare strumenti e soluzioni di monitoraggio del traffico di rete;
- Garantire una sicura gestione degli incidenti di sicurezza;
- Garantire lo smaltimento ed il riutilizzo sicuro delle attrezzature e dei supporti;
- Garantire la identificazione delle responsabilità per l'autorizzazione degli accessi fisici, il *workflow* per la concessione di tali permessi e gli step autorizzativi;
- Limitare gli accessi alle stanze server unicamente al personale autorizzato;
- Migliorare il processo di inventariazione dei beni e strumenti informatici allo scopo di tracciare e monitorare apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche;
- Informare gli utilizzatori dei sistemi informatici che i software per l'esercizio delle attività di loro competenza sono protetti dalle leggi sul diritto d'autore ed in quanto tali ne è vietata la duplicazione, la distribuzione, la vendita o la detenzione a scopo commerciale/imprenditoriale;
- Garantire che i contratti che regolano i rapporti con i fornitori delle presenti attività (servizi in outsourcing) prevedano apposite clausole che impongano:
  - la conformità dei software forniti a leggi e normative applicabili;
  - la manleva per la Società in caso di violazioni commesse dai fornitori del servizio stessi.
- Garantire che ai contratti che regolano i rapporti con i fornitori siano apposte clausole che richiamano gli adempimenti e le responsabilità derivanti dal Decreto 231 e dal rispetto dei principi fondamentali del Modello 231 e del Codice Etico e che indicano chiari effetti contrattuali in merito al mancato rispetto di detti adempimenti;
- Implementare meccanismi di tracciatura degli eventi di sicurezza sulle reti (ad es. accessi anomali per frequenza, modalità, temporalità);
- Garantire l'implementazione e la manutenzione delle reti telematiche mediante la definizione di responsabilità e modalità operative, di verifiche periodiche sul funzionamento delle reti e sulle anomalie riscontrate; inoltre, sia regolamentata l'esecuzione di attività periodiche di *vulnerability assessment* ed *ethical hacking*;
- Definire le responsabilità per la gestione delle reti;
- Nell'ambito della gestione di reti di fibra ottica spenta, ai fini di prevenire fenomeni di tipo corruttivo:
  - Identificare i soggetti che intrattengono rapporti con soggetti privati nell'ambito della gestione di reti di fibra ottica spenta;
  - Garantire la tracciabilità delle informazioni fornite e ricevute a/dai suddetti soggetti privati;
  - Garantire costantemente specifici flussi informativi verso l'OdV e riferimenti puntuali alle sezioni rilevanti del Codice Etico adottato dalla Società;

  - Garantire la corretta archiviazione della documentazione riguardante ogni singola attività prevista dal presente processo allo scopo di garantire la completa tracciabilità dello stesso.
- Garantire che nessun dipendente acceda in maniera abusiva ai sistemi informativi utilizzati dalla Pubblica Amministrazione o ne alteri in qualsiasi modo il funzionamento oppure intervenga con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico per ottenere e/o modificare indebitamente informazioni a vantaggio dell'azienda od a terzi;
- Informare adeguatamente i dipendenti della Società e gli altri soggetti, eventualmente autorizzati all'utilizzo dei Sistemi Informativi, come ad esempio i collaboratori esterni, dell'importanza di:
  - mantenere le proprie credenziali confidenziali e di non divulgare le stesse a soggetti terzi;
  - utilizzare correttamente i software e le banche dati in dotazione;
  - non utilizzare dati, immagini o altro materiale coperto dal diritto d'autore senza avere ottenuto le necessarie autorizzazioni dai propri superiori gerarchici secondo le indicazioni contenute nelle policy aziendali.
- Curare l'informativa diretta agli utilizzatori dei sistemi informatici volta a diffondere la consapevolezza che tutti i software forniti dalla Società sono protetti dalle leggi sul diritto d'autore ed in quanto tali ne è vietata la duplicazione, la distribuzione, la vendita o la detenzione a scopo commerciale/imprenditoriale.

È compito di tutti i Dipendenti assegnatari di strumenti hardware e software aziendali:
- Compilare ed accettare formalmente una "scheda di presa in carico" dove, previa elencazione di tutta la strumentazione hardware e software fornita, vengono descritte le condizioni d'uso che tutto il personale si impegna a rispettare;
- Rispettare gli obblighi ed i divieti esposti nella suesposta "scheda di presa in carico", ossia:
  - l'obbligo di utilizzare il PC per le sole esigenze di servizio;
  - l'obbligo di non cedere, in nessun caso, neppure in via temporanea, l'uso del PC a terzi, né a titolo oneroso, tenendo, in particolare, segreta la password per il collegamento da remoto alla rete aziendale, laddove previsto;
  - il divieto di istallare software non forniti da Romagna Acque, ancorché distribuiti gratuitamente, salvo preventiva autorizzazione dell'Amministratore di Sistema;
  - l'obbligo di conservare e custodire con cura e con la massima diligenza il PC provvedendo alla restituzione dello stesso nello stato attuale, salvo il normale deterioramento, non appena richiesto dalla Società e comunque non oltre il termine massimo da quest'ultima eventualmente fissato, senza possibilità di opporre eccezione alcuna;
  - l'obbligo di comunicare con la massima tempestività l'eventuale smarrimento e/o furto del PC informando in ogni caso la Società circa la natura e l'entità dei dati aziendali in esso memorizzati.
- Riconsegnare il materiale attraverso la compilazione di una scheda di "restituzione della dotazione informatica", e rispettare il divieto di criptare, riservare, rendere comunque inutilizzabili i dati contenuti nel PC oggetto di riconsegna.
- Connettere ai sistemi informatici di Romagna Acque solo i personal computer e le periferiche fornite dalla Società;
- Richiedere l'autorizzazione dell'Amministratore di Sistema per l'installazione di software non forniti dalla Società;
- Rispettare gli accordi contrattuali di licenza d'uso e, in generale, di tutte le leggi ed i regolamenti che disciplinano e tutelano il diritto d'autore;
- Non divulgare, cedere o condividere con personale interno o esterno a Romagna Acque le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti o terze parti;

- Segnalare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici aziendali o di terze parti, che potrebbero consentire l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere.

3.7. Codice etico, Piano Triennale di Prevenzione della Corruzione e della Trasparenza e principi di comportamento e di controllo

I Destinatari del Modello, ed in particolare i soggetti aziendali coinvolti nella presente area a rischio, così come identificati nei precedenti paragrafi, sono tenuti, nello svolgimento delle attività sensibili, a tenere un comportamento corretto e trasparente, in conformità a quanto previsto dalle previsioni di legge esistenti in materia, dal Modello 231 approvato dalla società, dal Codice Etico adottato dalla Società.
Romagna Acque persegue l'obiettivo del corretto utilizzo dei servizi informatici o telematici, in modo da garantire l'integrità e la genuinità dei dati trattati, a tutela degli interessi della Società e dei terzi, con particolare riferimento alle Autorità ed Istituzioni pubbliche.
La Società, a tal fine, adotta misure idonee ad assicurare che l'accesso ai dati telematici ed informatici avvenga nell'assoluto rispetto delle normative vigenti e della privacy dei soggetti eventualmente coinvolti ed in modo da garantire la riservatezza delle informazioni e far sì che il loro trattamento avvenga a cura di soggetti a ciò espressamente autorizzati, impedendo indebite intromissioni.
In particolare, la Società vieta:

- l'introduzione abusiva nei sistemi informatici o telematici protetti da misure di sicurezza;
- la distruzione, il deterioramento, la cancellazione o alterazione di informazioni, dati o programmi informatici altrui, dello Stato o di altro Ente pubblico;
- la produzione di documenti informatici falsi, sia privati che pubblici, aventi efficacia probatoria;
- l'installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi;
- la sottrazione, la riproduzione, la diffusione o la consegna abusiva di codici, parole chiavi o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza.

3.8. Compiti ed attività dell'Organismo di Vigilanza e del Responsabile della Prevenzione della Corruzione e della Trasparenza

In materia di compiti ed attività dell'Organismo di Vigilanza e del Responsabile per l'attuazione del Piano Triennale di Prevenzione della Corruzione e della Trasparenza si rimanda alla specifica sezione della Parte Generale del Modello.

3.9. Sistema disciplinare

In materia di sistema disciplinare (sanzionatorio) si rimanda alla specifica sezione della Parte Generale del Modello 231 e dell'Allegato C – Sistema Sanzionatorio.

3.10. Archiviazione della documentazione

Tutta la documentazione prodotta nell'ambito delle attività disciplinate nel presente Protocollo è conservata a cura dei responsabili delle funzioni aziendali coinvolte secondo le modalità vigenti in azienda e nel rispetto delle tempistiche previste dalle normative vigenti.

3.1. Comunicazione, formazione e informazione

In materia di comunicazione, formazione e informazione si rimanda alla specifica sezione della Parte Generale del Modello 231.

4. Area a rischio n. 2: "Gestione dei dati sensibili *ex* D.lgs. n.196/2003"

4.1. Funzioni aziendali coinvolte

Le funzioni aziendali della Società coinvolte nell'attività di gestione dei dati sensibili *ex* D.Lgs. n. 196/2003 sono rappresentate dalle seguenti:
- Consiglio di Amministrazione
- Presidente del Consiglio di Amministrazione
- Direttore generale;
- Responsabile del trattamento dei dati rilevanti ai sensi del Decreto Privacy;
- Incaricati al trattamento dei dati rilevanti ai sensi del Decreto Privacy;
- Area Servizi – Servizi Sistemi Informativi e Telecomunicazioni;
- Area Amministrazione, Finanza, Pianificazione e Controllo, Personale e Organizzazione;
- Amministratore di Sistema.

4.2. Attività sensibili

Nell'ambito della sopra indicata area a rischio n. 1 si individuano le specifiche attività sensibili di seguito elencate:
- Selezione, assunzione e gestione del personale aziendale ;
- Gestione dei sistemi informatici ;
- Gestione degli accessi logici ;
- Gestione del software ;
- Gestione della rete e dell'hardware ;
- Gestione della sicurezza fisica ;
- Gestione outsourcing IT ;
- Utilizzo della postazione di lavoro ;
- Installazione, manutenzione, aggiornamento e gestione di software di soggetti pubblici o forniti per conto di soggetti pubblici ;
- Gestione di reti di fibra ottica spenta .

4.3. Reati astrattamente ipotizzabili

Si elencano di seguito i possibili reati configurabili con riferimento alle attività sensibili individuate nella presente area a rischio:
2. Documenti informatici (art. 491 *bis* c.p.)
6. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 *quater* c.p.)
7. Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 *quinquies* c.p.)
8. Danneggiamento di informazioni, dati e programmi informatici (art. 635 *bis* c.p.)

4.4. Esempi di possibili modalità di realizzazione del reato e relative finalità

A titolo esemplificativo, con riferimento ai reati informatici, si potrebbero configurare le seguenti modalità di realizzazione di reato:

2. 6. Diffondere, utilizzare senza idonea autorizzazione dati sensibili relativi a dipendenti, clienti, fornitori o altri Destinatari;
7. 8. Gestire il sistema informativo in modo da consentire violazioni dello stesso tali da causare diffusione o utilizzo illecito di dati sensibili in esso conservati.

4.5. Controlli chiave necessari a fronte dei rischi rilevati

Al fine di prevenire la commissione dei reati indicati nei precedenti paragrafi, la Società ha predisposto e implementato appositi presidi organizzativi e di controllo.
Tutte le funzioni coinvolte in tali attività sono tenute ad osservare le disposizioni di legge esistenti in materia, le prescrizioni previste dal D.lgs. n. 231/2001, nonché quanto previsto dal Modello di organizzazione, gestione e controllo e dal Codice Etico.
Di seguito sono riportati i controlli chiave necessari a fronte dei rischi rilevati nell'attività di gestione dei dati sensibili ai sensi del Decreto Privacy:

- Compiere e sottoscrivere ogni atto o dichiarazione dovuti dalla società, quale Titolare di tutti i trattamenti aziendali dei dati rilevanti ai sensi del Decreto Privacy.;
- Conferire la Responsabilità al trattamento dei dati personali ai sensi del Codice in materia di dati personali e del Disciplinare tecnico in materia di misure minime di sicurezza di cui al Decreto Privacy tramite sottoscrizione di apposita Lettera di Incarico;
- Garantire che il trattamento di dati personali con strumenti elettronici sia consentito ai soli incaricati dotati di credenziali di autenticazione (*username* e password);Garantire che tutte le misure di sicurezza riguardanti i dati personali siano applicate;
- Individuare, nominare e affidare per iscritto la responsabilità al trattamento dei dati personali ai sensi del Codice in materia di dati personali e del Disciplinare tecnico in materia di misure minime di sicurezza di cui al Decreto Privacy tramite sottoscrizione di apposita Lettera di Incarico;
- Nominare gli Incaricati del trattamento dei dati e provvedere a rinnovare annualmente tale nomina;
- Raccogliere i dati personali dei dipendenti fornendo l'informativa all'interessato o alla persona presso cui si raccolgono i dati, secondo quanto stabilito dall'art. 13 del Decreto Privacy (in forma orale oppure utilizzando apposita modulistica predisposta dal Titolare);
- Garantire che il trattamento di dati personali con strumenti elettronici sia consentito agli incaricati dotati di credenziali di autenticazione che ammettano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti;
- Prevedere che i codici identificativi (*user-id*) per l'accesso alle applicazioni ed alla rete siano individuali ed univoci;
- Impartire istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento;
- Verificare periodicamente, e comunque almeno annualmente, la sussistenza delle condizioni per la conservazione dei profili di autorizzazione;
- Garantire che i dati personali oggetto di trattamento siano:
  - trattati in modo lecito e secondo correttezza;

  - raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
  - esatti e, se necessario, aggiornati;
  - pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
  - conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.
- Redigere ed aggiornare ad ogni variazione l'elenco delle sedi in cui vengono trattati i dati;
- Redigere ed aggiornare ad ogni variazione l'elenco dei dati oggetto di trattamento;
- Definire e modificare con cadenza semestrale le modalità di accesso ai locali e le misure da adottare per la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- Se il trattamento dei dati è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più incaricati della gestione e della manutenzione degli strumenti elettronici e della custodia delle copie delle credenziali e delle copie di sicurezza delle banche dati;
- Generare, sostituire e invalidare, in relazione agli strumenti e alle applicazioni informatiche utilizzate, le parole chiave ed i codici di accesso personali da assegnare agli incaricati del trattamento dei dati, nel rispetto delle massime misure di sicurezza;
- Adottare adeguati programmi antivirus, firewall e altri strumenti software o hardware atti a garantire la massima misura di sicurezza nel rispetto di quanto dettato dal Decreto Privacy ed utilizzando le conoscenze acquisite in base al progresso tecnico;
- Controllare l'efficienza dei sistemi tecnici adottati e redigere un apposito verbale, riportante i nominativi dei partecipanti al controllo, i riscontri e le verifiche effettuate, i parametri e gli accorgimenti proposti per migliorare la sicurezza;
- Prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di *back up*;
- Assicurarsi della qualità delle copie di back up dei dati e della loro conservazione in luogo adatto e sicuro;
- Provvedere che sia prevista la disattivazione dei codici identificativi personali, in caso di perdita della qualità che consentiva all'utente o incaricato l'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei Codici identificativi personali per oltre 6 mesi;
- Indicare al personale competente o provvedere direttamente alla distruzione e smaltimento dei supporti informatici di memorizzazione logica o alla cancellazione dei dati per il loro reimpiego;
- Provvedere alla nomina di uno o più Custodi delle password per l'accesso ai dati archiviati nei sistemi di elaborazione dati;
- Curare l'archiviazione delle lettere di Incarico rilasciate dalla Società;
- Custodire e conservare i supporti utilizzati per le copie dei dati;
- Raccogliere i dati personali dei dipendenti, fornendo l'informativa all'interessato o alla persona presso cui si raccolgono i dati, secondo quanto stabilito dall'art. 13 del Decreto Privacy (in forma orale oppure utilizzando apposita modulistica predisposta dal Titolare);
- Adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

4.6. Sistema autorizzativo e segregazione delle funzioni

La Società, con riferimento all'area a rischio in oggetto, ha assegnato le seguenti responsabilità, rispondendo a criteri di segregazione delle funzioni, al fine di consentire un efficace monitoraggio.

È compito dell'Amministratore Delegato:

- Compiere e sottoscrivere ogni atto o dichiarazione dovuti dalla società, quale Titolare di tutti i trattamenti aziendali dei dati rilevanti ai sensi del Decreto Privacy;
- Conferire la Responsabilità al trattamento dei dati personali ai sensi del Codice in materia di dati personali e del Disciplinare tecnico in materia di misure minime di sicurezza di cui al Decreto Privacy tramite sottoscrizione di apposita Lettera di Incarico;
- Garantire che il trattamento di dati personali con strumenti elettronici sia consentito ai soli incaricati dotati di credenziali di autenticazione (*username* e password);
- Garantire che tutte le misure di sicurezza riguardanti i dati personali siano applicate;
- Individuare, nominare e affidare per iscritto la responsabilità al trattamento dei dati personali ai sensi del Codice in materia di dati personali e del Disciplinare tecnico in materia di misure minime di sicurezza di cui al Decreto Privacy tramite sottoscrizione di apposita Lettera di Incarico.

È compito della Funzione "Sistemi Informativi e Telecomunicazioni":

- Prevedere che i codici identificativi (*user-id*) per l'accesso alle applicazioni ed alla rete siano individuali ed univoci.

È compito dei Responsabili del trattamento dei dati rilevanti ai sensi del Decreto Privacy, con l'ausilio dell'Amministratore di Sistema:

- Nominare gli Incaricati del trattamento dei dati e provvedere a rinnovare annualmente tale nomina;
- Impartire istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento;
- Verificare periodicamente, e comunque almeno annualmente, la sussistenza delle condizioni per la conservazione dei profili di autorizzazione;
- Garantire che i dati personali oggetto di trattamento siano:
  - trattati in modo lecito e secondo correttezza;
  - raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
  - esatti e, se necessario, aggiornati;
  - pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
  - conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.
- Redigere ed aggiornare ad ogni variazione l'elenco delle sedi in cui vengono trattati i dati;
- Redigere ed aggiornare ad ogni variazione l'elenco dei dati oggetto di trattamento;
- Definire e modificare con cadenza semestrale le modalità di accesso ai locali e le misure da adottare per la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- Se il trattamento dei dati è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più incaricati della gestione e della manutenzione degli strumenti elettronici e della custodia delle copie delle credenziali e delle copie di sicurezza delle banche dati;
- Generare, sostituire e invalidare, in relazione agli strumenti e alle applicazioni informatiche utilizzate, le parole chiave ed i codici di accesso personali da assegnare agli incaricati del trattamento dei dati, nel rispetto delle massime misure di sicurezza;
- Adottare adeguati programmi *antivirus*, *firewall* e altri strumenti software o hardware atti a garantire la massima misura di sicurezza nel rispetto di quanto dettato dal Decreto Privacy ed utilizzando le conoscenze acquisite in base al progresso tecnico;

- Controllare l'efficienza dei sistemi tecnici adottati e redigere un apposito verbale, riportante i nominativi dei partecipanti al controllo, i riscontri e le verifiche effettuate, i parametri e gli accorgimenti proposti per migliorare la sicurezza;
- Prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di *back up*;
- Assicurarsi della qualità delle copie di *back up* dei dati e della loro conservazione in luogo adatto e sicuro;
- Provvedere che sia prevista la disattivazione dei codici identificativi personali, in caso di perdita della qualità che consentiva all'utente o incaricato l'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei Codici identificativi personali per oltre 6 mesi;
- Indicare al personale competente o provvedere direttamente alla distruzione e smaltimento dei supporti informatici di memorizzazione logica o alla cancellazione dei dati per il loro reimpiego;
- Provvedere alla nomina di uno o più Custodi delle password per l'accesso ai dati archiviati nei sistemi di elaborazione dati;
- Curare l'archiviazione delle Lettere di Incarico rilasciate dalla Società;
- Custodire e conservare i supporti utilizzati per le copie dei dati.

È compito degli Incaricati del trattamento dei dati rilevanti ai sensi del Decreto Privacy:

- Raccogliere i dati personali dei dipendenti, fornendo l'informativa all'interessato o alla persona presso cui si raccolgono i dati, secondo quanto stabilito dall'art. 13 del Decreto Privacy (in forma orale oppure utilizzando apposita modulistica predisposta dal Titolare);
- Adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

4.7. Codice etico e principi di comportamento e di controllo

I Destinatari del Modello, ed in particolare i soggetti aziendali coinvolti nella presente area a rischio, così come identificati nei precedenti paragrafi, sono tenuti, nello svolgimento delle attività sensibili, a tenere un comportamento corretto e trasparente, in conformità a quanto previsto dalle previsioni di legge esistenti in materia, dal Modello 231 approvato dalla società, dal Codice Etico adottato dalla Società.
Romagna Acque garantisce che il trattamento dei dati personali sia posto in essere nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali e sensibili.
In particolare è fatto obbligo del personale di Romagna Acque di assicurare la riservatezza richiesta dalle circostanze per ciascuna notizia appresa in ragione della propria funzione lavorativa.
In aggiunta, i dati personali oggetto di trattamento devono essere:

- trattati in modo lecito e secondo correttezza;
- raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
- esatti e, se necessario, aggiornati;
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

Fermo restando il divieto di divulgare notizie attinenti all'organizzazione o di farne uso in modo da poter recare ad essa pregiudizio, si dovrà:

- acquisire e trattare solo i dati necessari ed opportuni per lo svolgimento delle proprie funzioni;

- acquisire e trattare i dati stessi solo all'interno di specifiche procedure;
- conservare, per il tempo stabilito dalla legge, i dati stessi in modo che venga impedito che altri non autorizzati ne prendano conoscenza;
- comunicare i dati stessi nell'ambito di procedure prefissate e/o su esplicita autorizzazione delle posizioni superiori e/o funzioni competenti, e comunque, in ogni caso, dopo essersi assicurato circa la divulgabilità nel caso specifico dei dati;
- assicurarsi che non sussistano vincoli assoluti o relativi alla divulgabilità delle informazioni riguardanti i terzi collegati a Romagna Acque da un rapporto di qualsiasi natura e, se del caso, ottenere il loro consenso;
- associare i dati stessi con modalità tali da consentire a qualsiasi soggetto autorizzato ad avervi accesso, di trarne agevolmente un quadro il più possibile preciso, esauriente e veritiero.

4.8. Compiti ed attività dell'Organismo di Vigilanza e del Responsabile della Prevenzione della Corruzione e della Trasparenza

In materia di compiti ed attività dell'Organismo di Vigilanza e del Responsabile della Prevenzione della Corruzione si rimanda alla specifica sezione della Parte Generale del Modello.

.

4.9. Sistema disciplinare

In materia di sistema disciplinare (sanzionatorio) si rimanda alla specifica sezione della Parte Generale del Modello 231 e dell'Allegato C – Sistema Disciplinare.

4.10. Archiviazione della documentazione

Tutta la documentazione prodotta nell'ambito delle attività disciplinate nel presente protocollo è conservata a cura dei responsabili delle funzioni aziendali coinvolte secondo le modalità vigenti in azienda e nel rispetto delle tempistiche previste dalle normative vigenti.

4.1. Comunicazione, formazione e informazione

In materia di comunicazione, formazione e informazione si rimanda alla specifica sezione della Parte Generale del Modello 231.

4.2. Flussi informativi verso l'Organismo di Vigilanza ed il Responsabile della Prevenzione della Corruzione e della Trasparenza

Al fine di consentire all'Organismo di Vigilanza di vigilare sull'efficace funzionamento e sull'osservanza del Modello e di curarne l'aggiornamento è necessario che sia definito ed attuato un costante scambio di informazioni tra i destinatari del Modello e l'Organismo di Vigilanza stesso.

In particolare, nel Modello 231 adottato dalla Società vengono individuate due tipologie di flussi informativi diretti all'OdV:

- Segnalazioni;
- Flussi informativi periodici

Per ulteriori informazioni in merito ai suddetti flussi informativi si rinvia alla Parte Generale del Modello 231; di seguito i flussi informativi implementati per il Protocollo "Gestione sistemi informativi e sicurezza dati".

5. Report specifico dei flussi informativi verso l'Organismo di Vigilanza ed il Responsabile della Prevenzione della Corruzione e della Trasparenza

Protocollo 231.INF – Gestione dei sistemi informativi e sicurezza dati			
Area a rischio	**Flussi informativi**	**Periodicità**	***Key Officer***
N.1 Gestione dei sistemi informativi aziendali	***Report* aventi ad oggetto:** – eventuali incidenti IT verificatisi, cause, relativi processi di risposta attivati e risultati ottenuti; – eventuali interventi di modifica sui sistemi informativi realizzati, motivazioni e risultati ottenuti; – eventuali autorizzazioni all'installazione di software diversi da quelli messi a disposizione dalla Società rilasciate, motivazioni e risultati ottenuti; – controlli e verifiche periodiche sull'efficienza del sistema e risultati ottenuti, con particolare evidenza su scostamenti rispetto alle previsioni o standard di riferimento; – riepilogo dei casi di eventuali utilizzi illegittimi, da parte del personale, delle attrezzature software e hardware ricevute in dotazione rilevati nel corso del periodo e tempestivamente segnalate nei report delle "INFORMAZIONI NON ORDINARIE", con esito della	**Annuale**	**Responsabile della Funzione "Sistemi Informativi e Telecomunicazioni"**

	verifica effettuata, rimedi, risultati ottenuti ed evidenze di applicazioni del sistema sanzionatorio; – ogni deroga alle procedure di processo decisa in caso di emergenza o di impossibilità temporanea di attuazione, indicando la motivazione, e ogni anomalia significativa riscontrata, nonché i risultati. – esecuzione, regolarità, adesione, validità e risultati del programma formativo, in funzione di un'adeguata formazione rispetto alle caratteristiche aziendali e del rispetto della normativa vigente. – Segnalare le anomalie riscontrate nell'esecuzione dei contratti connessi alla gestione di reti di fibra ottica spenta nonché alla gestione della telefonia cellulare e delle postazioni radio.		
N. 2 Gestione dei dati sensibili *ex* D.lgs. n. 196/2003	***Report aventi ad oggetto:*** – eventuali incidenti relativi alla sicurezza dei dati, cause e rimedi; – verificare modalità di accesso ai locali e misure da adottare definite per la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità e segnalazione delle anomalie	**Annuale**	**Responsabile della Funzione "Sistemi Informativi e Telecomunicazioni"**

	Report aventi ad oggetto: – esiti delle verifiche periodiche svolte per garantire la sussistenza delle condizioni per la conservazione dei profili di autorizzazione; – formazione/informazione erogata in materia di tutela della privacy e sulle procedure aziendali in essere;	**Annuale**	**Responsabile della Funzione "Sistemi Informativi e Telecomunicazioni"**

INFORMAZIONI NON ORDINARIE			
Area	**Flussi informativi**	**Periodicità**	***Key Officer***
Generale	***Report* aventi ad oggetto:** – eventuali non conformità e rimedi assunti relativi all'applicazione del flusso; – eventuali non conformità e rimedi assunti rispetto a prassi e procedure aziendali; – eventuali non conformità e rimedi assunti rispetto alle disposizioni del Codice Etico; – eventuali non conformità e rimedi assunti rispetto al D.Lgs. n. 231/2001 e al Modello adottato; – eventuali deroghe alle procedure di processo decise in caso di emergenza o di impossibilità temporanea di attuazione, motivazioni e risultati relativi; – eventuali utilizzi illegittimi, da parte del personale, delle attrezzature software e hardware ricevute in dotazione,	**Al riscontro della non conformità**	**Responsabile della Funzione "Sistemi Informativi e Telecomunicazioni"**

	con esito della verifica effettuata, rimedi, risultati ottenuti ed evidenze di applicazioni del sistema sanzionatorio.		