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 sistemi informative e Sicurezza dati"	1.0	18/06/2014	Prima emissione	
Protocollo di controllo "Gestione dei sistemi informative e Sicurezza dati"	Rev. 01		Rev. 01 dell'emissione del 18.06.2014	

E M I S S I O N E E M O D I F I C H E				
Revisioni	***Data***	***Redatto:***	***Verificato:***	***Approvato:***
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**
Rev. 02 *	**31.03.2025**	**Servizio Compliance, RPCT, Comunicazione e Relazioni esterne**	**Organismo di Vigilanza**	**Delibera CdA n. 30 del 31.03.2025**

***Aggiornamento normativo; aggiornamento Flussi informativi e recepimento organigramma del 01.01.2025**

Indice

1. Definizioni

- **CdA:** Consiglio di Amministrazione di Romagna Acque – Società delle Fonti S.p.A.
- **Codice dei Contratti Pubblici:** Decreto Legislativo 31 marzo 2023, n. 36 e successive modifiche ed integrazioni
- **Decreto 231:** Decreto Legislativo 8 giugno 2001, n. 231
- **Legge 190/2012 o Legge Anticorruzione:** Legge del 6 Novembre 2012 n. 190 "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione", e relativi provvedimenti applicativi
- **Modello 231:** Modello di organizzazione e gestione ex articolo 6 del Decreto Legislativo 8 giugno 2001, n. 231
- **OdV:** Organismo di Vigilanza ex articolo 6 del Decreto Legislativo 8 giugno 2001, n. 231
- **PTPCT:** Piano Triennale di Prevenzione della Corruzione e della Trasparenza
- **RPCT:** Responsabile per l'attuazione del Piano di Prevenzione della Corruzione e della Trasparenza
- **RUP:** Responsabile unico del progetto per le fasi di programmazione, progettazione, affidamento e per l'esecuzione di ciascuna procedura soggetta al codice dei contratti pubblici ex d.lgs. 31.03.2023, n. 36
- **Soglia Comunitaria:** Soglia del valore dell'affidamento determinate in ossequio alle disposizioni vigenti
- **Società:** Romagna Acque – Società delle Fonti S.p.A.
- **Romagna Acque:** Romagna Acque – Società delle Fonti S.p.A.

2. Reati

La gestione dei sistemi informativi e sicurezza dei dati rappresenta un'attività trasversale a tutti i sistemi gestionali dell'impresa. In particolare, la gestione degli approvvigionamenti potrebbe configurare attività a rischio di commissione dei reati-presupposto *ex* d.lgs. 231 del 2001 e di violazione di norme anticorruzione, indicati alle seguenti sezioni della Parte speciale.

- PS Sezione II – "Art. 24 - Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture" e "Art. 25 - Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio", integrati ai sensi della L. n. 190 del 2012
- PS Sezione IV – "Art. 24-*bis* – Delitti informatici e trattamento illecito di dati"
- PS Sezione III – "Art. 25-*octies* - Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio" e "Art. 25-*octies*.1 - Delitti in materia di strumenti di pagamento diversi dai contanti"

Un maggiore dettaglio in merito ai reati-presupposto ipoteticamente commissibili, associati alle relative parti speciali e con indicazione degli indici di rischio pre e post adozione del MOG, è disponibile nei file/documenti allegati estratti dal risk assessment e afferenti al protocollo in oggetto.

2.1. Esempi di possibili modalità di realizzazione dei reati e relative finalità

A titolo puramente esemplificativo, senza alcuna pretesa di esaurire la vasta casistica possibile e con riferimento solo ad alcune ipotesi di reato elencate, si potrebbero configurare, per sommi capi, le seguenti modalità di commissione del reato da parte dei soggetti indicati all'art. 5 del d.lgs. 231/2001 e dalla L. 190/2012.

2.1.1. INDEBITA PERCEZIONE DI EROGAZIONI, TRUFFA IN DANNO DELLO STATO, DI UN ENTE PUBBLICO O DELL'UNIONE EUROPEA O PER IL CONSEGUIMENTO DI EROGAZIONI PUBBLICHE, FRODE INFORMATICA IN DANNO DELLO STATO O DI UN ENTE PUBBLICO E FRODE NELLE PUBBLICHE FORNITURE (AI SENSI DELL'ART. 24 DEL D.LGS. 231/2001 E L. 190/2012)

Frode informatica (art. 640-*ter* c.p.) **in danno dello Stato o di altro ente pubblico**

Il reato si configura nel caso in cui, chiunque, alterando il funzionamento di un sistema informatico o telematico o manipolando i dati in esso contenuti (attraverso un intervento non autorizzato, effettuato con qualsiasi modalità), si ottenga un ingiusto profitto arrecando danno a terzi.
Nel caso di intervento non autorizzato è compresa sia l'ipotesi in cui un soggetto abilitato e/o autorizzato a determinati interventi approfitti della situazione per porre in essere comportamenti diversi da quelli rientranti nella propria sfera operativa, che quella dell'agente privo, anche in astratto, della possibilità di intervento.
L'alterazione fraudolenta del sistema può essere la conseguenza di un intervento rivolto sia alla componente meccanica dell'elaboratore, sia al software.
Per la configurabilità dell'aggravante dell'abuso della qualità di operatore di sistema è richiesto che il soggetto attivo rivesta la qualità di operatore di sistema, e cioè che sia stabilmente ed ufficialmente preposto all'utilizzo del sistema informatico o telematico in virtù di un rapporto privatistico.
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.
Si riportano di seguito le esemplificazioni relative alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società – attraverso un proprio operatore – agendo per sé o per altri, si procura un profitto ingiusto, provocando allo Stato o a qualsiasi altro ente pubblico un danno, mediante i seguenti comportamenti:
  - alterazione del funzionamento di un sistema informatico o telematico dello Stato o di un diverso ente pubblico tramite qualsiasi mezzo;
  - intervento non autorizzato su dati/informazioni/programmi contenuti in un sistema informatico o telematico dello Stato o di un diverso ente pubblico tramite qualsiasi mezzo;
  - intervento non autorizzato su dati/informazioni/programmi pertinenti a un sistema informatico o telematico dello Stato o di un diverso ente pubblico tramite qualsiasi mezzo.
- La Società – mediante un proprio operatore - altera i dati presenti nei registri informatici per far risultare esistenti in capo ad un proprio cliente condizioni essenziali per la partecipazione a gare indette dalla Pubblica Amministrazione.
- La Società, nel proprio interesse o vantaggio, altera i dati relativi ai dipendenti con disabilità in servizio attivo, al fine di aggiudicarsi un contributo pubblico, così realizzando un ingiusto profitto in favore della società con danno in capo all'ente stesso.
- La Società, nel proprio interesse o vantaggio, altera i dati relativi ai dipendenti che hanno usufruito di una determinata iniziativa formativa al fine di aggiudicarsi un contributo pubblico, così realizzando un ingiusto profitto in favore della Società con danno in capo all'ente stesso.
- La Società – mediante un proprio operatore - altera i registri informatici della Pubblica Amministrazione per far risultare esistenti condizioni essenziali per la partecipazione a gare (es. iscrizione in albi) ovvero per la successiva produzione di

documenti attestanti fatti e circostanze inesistenti o, ancora, per modificare dati fiscali/previdenziali di interesse dell'azienda, già trasmessi all'Amministrazione stessa.

2.1.2. DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI (AI SENSI DELL'ART. 24-BIS, D.LGS. 231 DEL 2001)

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

La norma contempla che "*se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti gli atti pubblici*.".

Il testo della norma del codice penale fa riferimento al Capo III "Della falsità in atti" contenuto nel Titolo VII "Dei delitti contro la fede pubblica" del Libro II del codice penale e richiama i seguenti articoli di quest'ultimo:

- Art. 476. Falsità materiale commessa dal pubblico ufficiale in atti pubblici;
- Art. 477. Falsità materiale commessa da pubblico ufficiale in certificati o autorizzazioni amministrative;
- Art. 478. Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti;
- Art. 479. Falsità ideologica commessa dal pubblico ufficiale in atti pubblici;
- Art. 480. Falsità ideologica commessa dal pubblico ufficiale in certificati o in autorizzazioni amministrative;
- Art. 481. Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità;
- Art. 482. Falsità materiale commessa dal privato;
- Art. 483. Falsità ideologica commessa dal privato in atto pubblico;
- Art. 484. Falsità in registri e notificazioni;
- Art. 487. Falsità in foglio firmato in bianco. Atto pubblico;
- Art. 488. Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali;
- Art. 489. Uso di atto falso;
- Art. 490. Soppressione, distruzione e occultamento di atti veri;
- Art. 492. Copie autentiche che tengono luogo degli originali mancanti;
- Art. 493. Falsità commesse da pubblici impiegati incaricati di un servizio pubblico.

Alcuni di questi reati possono non essere commissibili nell'attività svolta dalla Società.

Si riportano di seguito alcune esemplificazioni relative alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria.

- La Società, agendo quale pubblico ufficiale, forma, in tutto o in parte, un atto falso o altera un atto vero.
- La Società, agendo quale pubblico ufficiale, contraffà o altera certificati o autorizzazioni amministrative, ovvero, mediante contraffazione o alterazione, fa apparire adempiute le condizioni richieste per la loro validità.
- La Società, agendo quale pubblico ufficiale, supponendo esistente un atto pubblico o privato, ne simula una copia e la rilascia in forma legale, ovvero rilascia una copia di un atto pubblico o privato diversa dall'originale.
- La Società, agendo quale pubblico ufficiale e ricevendo o formando un atto nell'esercizio delle sue funzioni, attesta falsamente che un fatto è stato da essa compiuto o è avvenuto in sua presenza, o attesta come da essa ricevute dichiarazioni non rese, ovvero omette o altera dichiarazioni da essa ricevute, o comunque attesta falsamente fatti dei quali l'atto è destinato a provare la verità.
- La Società, agendo quale pubblico ufficiale, attesta falsamente, in certificati o autorizzazioni amministrative, fatti dei quali l'atto è destinato a provare la verità.
- La Società, agendo quale soggetto privato, forma, in tutto o in parte, un atto falso o altera un atto vero.
- La Società, agendo in qualità di pubblico ufficiale ed abusando di un foglio firmato in bianco, del quale abbia il possesso per ragione del suo ufficio o per un titolo che importa l'obbligo o la facoltà di riempirlo, vi scrive o vi fa

scrivere un atto pubblico diverso da quello a cui era obbligata o autorizzata.
- La Società senza essere concorsa nella falsità, fa uso di un atto pubblico falso.
- La Società, in tutto o in parte, distrugge, sopprime od occulta un atto pubblico vero.

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

È punito sia colui che si introduce abusivamente, cioè senza il consenso del titolare del diritto di gestire l'accesso al sistema informatico o telematico munito di sistemi di sicurezza, sia colui che permane in collegamento con il sistema stesso continuando a fruire dei servizi resi o ad accedere alle informazioni in esso custodite, nonostante il titolare abbia esercitato, sia pur tacitamente, il diritto di impedire l'accesso.

Si potrebbero configurare le seguenti modalità di commissione del reato.
- La Società o il dipendente 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 diritto di escluderla.

Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-*quater* c.p.)

Questa norma completa la tutela prevista dalla precedente e punisce l'abusiva produzione, detenzione, importazione, diffusione e/o acquisizione in qualunque modo (comprensivo dell'autonoma elaborazione) dei mezzi o codici di accesso, da parte di soggetti non legittimati ad inserirsi nel sistema informatico o telematico altrui, vanificando l'ostacolo costituito dalle misure di protezione.
A titolo esemplificativo, la commissione dei reati previsti potrebbe derivare dalle seguenti condotte.
- La Società, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica – consegna mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, 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.

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

La norma intende tutelare sia la libertà di comunicare che il diritto alla riservatezza delle comunicazioni. È così estesa la tutela apprestata alle comunicazioni telegrafiche e telefoniche dall'art. 617 c.p. anche alle comunicazioni informatiche e telematiche.
Il reato può essere commesso secondo le seguenti modalità.
- La Società fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe.

Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-*quinquies* c.p.)

La condotta consiste nel procurarsi, detenere, produrre, riprodurre, diffondere, importare, comunicare, consegnare, mettere in altro modo a disposizione di altri e/o installare di strumenti idonei ad intercettare, impedire o interrompere le comunicazioni; non è necessario il loro effettivo funzionamento, a meno che non si tratti di mezzi tecnici assolutamente incapaci a realizzare una qualsiasi interferenza.
Si possono configurare le seguenti modalità di commissione del reato.
- La Società, fuori dei casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi.

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

Oltre alle ipotesi tradizionali di "distruzione" e di "deterioramento", sono state aggiunte a questa norma anche quelle di "cancellazione, alterazione e soppressione" delle informazioni, dei dati o dei programmi informatici altrui.
Per individuare, nell'ipotesi in esame, la persona offesa dal reato ed interpretare il concetto di altruità, non si può fare riferimento al concetto giuridico di possesso dei dati, delle informazioni o dei programmi, poiché caratterizzati dalla immaterialità. La cerchia degli aventi diritto all'integrità dei dati, delle informazioni e dei programmi dovrà essere determinata alla stregua della pluralità degli interessi giuridicamente rilevanti, di natura obbligatoria, anziché "reale", che su di essi possono convergere.
Nel caso di danneggiamento di programmi, possono essere considerate persone offese il legittimo utilizzatore, il concedente, il proprietario, l'operatore del sistema, nonché i *partners* commerciali o di lavoro di un'impresa o di un professionista, rispetto ad informazioni e dati da essi forniti per determinate finalità operative.
Il reato può essere commesso secondo le seguenti modalità.

- La Società distrugge, deteriora, cancella, altera o sopprime sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui.

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 disposto della norma si allinea con il contenuto di cui all'art. 635-bis, con la differenza che, in questo caso, si parla di danneggiamento di dati di pubblica utilità. Fin dalla rubrica, infatti, si parla di sistemi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, la quale viene riferita ad informazioni, dati o programmi informatici.
Si riporta di seguito l'esemplificazione relativa alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria.

- La Società 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 (Art 635-ter c.p.).

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

La norma in questione contempla come condotte penalmente rilevanti, oltre a quelle previste dall'art. 635-bis c.p., anche l'introduzione o la trasmissione di dati, informazioni o programmi, se tali attività conducono alla distruzione, al danneggiamento o comunque all'inservibilità totale o parziale di sistemi informatici o telematici altrui. Vi è, inoltre, l'ulteriore ipotesi alternativa, realizzabile quando le condotte poste in essere ostacolano gravemente il funzionamento del sistema.
Tra le varie, il reato può essere commesso secondo la seguente modalità.

- La Società, mediante le condotte di cui all'art. 635-bis c.p. ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento.

Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 635-*quater.1* c.p.)

La norma è stata introdotta dalla Legge n. 90 del 2024 e si occupa della detenzione, diffusione e installazione abusiva di apparecchiature o programmi informatici con l'intento di danneggiare sistemi informatici o telematici.
Un esempio di commissione di questo reato riguarda la manipolazione informatica che può comportare l'alterazione o la cancellazione di dati originali, rendendo inservibili le informazioni veritiere: un dipendente, con accesso alle informazioni sensibili, modifica i dati nel sistema informatico dell'azienda per far apparire i risultati migliori di quanto non siano realmente.

Danneggiamento di sistemi informatici o telematici di pubblico interesse (art. 635-*quinquies* c.p.)
La formulazione dell'articolo si allinea alla enunciazione dell'art. 635-quater c.p. estendendola all'ambito pubblicistico. Si ritiene che questa formula generica sia idonea ad abbracciare tutte le situazioni menzionate nella norma, non chiedendo come condizione necessaria l'utilizzazione effettiva da parte di un soggetto pubblico.
Si riporta di seguito l'esemplificazione relativa alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società, mediante le condotte di cui all'art. 635-bis c.p. ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia o rende, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ne ostacola gravemente il funzionamento.

Estorsione (art. 629, c. 3, c.p.)

Il comma 1-bis dell'art. 24-bis prevede una sanzione pecuniaria in relazione alla commissione del reato di estorsione informatica.

Tra le varie, il reato può essere commesso secondo la seguente modalità.

- Un dipendente della Società raccoglie informazioni su fornitori attraverso accessi non autorizzati ai loro sistemi. Sebbene l'intenzione fosse quella di ottenere informazioni per migliorare la strategia aziendale, il dipendente, per ottenere migliori performance personali aziendali, comunica ai fornitori che ha accesso ai loro dati e li minaccia indirettamente chiedendo vantaggi commerciali in cambio del silenzio.

Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies)

Non si ritiene reato commissibile da parte della Società.

Perimetro di sicurezza nazionale cibernetica (art. 1 - Decreto legge 21 settembre 2019, n. 105 convertito in legge con modifiche dalla legge 18 novembre 2019, n. 133)

Non si ritiene reato commissibile da parte della Società.

2.1.3. DELITTI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI E TRASFERIMENTO FRAUDOLENTO DI VALORI (AI SENSI DELL'ART. 24-OCTIES.1, D.LGS. 231 DEL 2001)

I reati richiamati dal c. 2 dell'art. 25-octies.1 del decreto sono la "*detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti*", previsto dall'art. 493-quater c.p. e la *frode informatica*, previsto dall'art. 640-ter c.p., quest'ultimo già visto in precedenza.

La norma, prevista dall'art. 493-quater c.p., è stata introdotta nel nostro ordinamento per adeguarsi alla normativa europea. Essa mira al contrasto del fenomeno delle frodi nei pagamenti elettronici già nella sua fase preparatoria, prima che il danno si verifichi effettivamente. Il legislatore ha quindi voluto colpire non solo chi materialmente commette la frode, ma anche chi fornisce gli strumenti necessari per realizzarla.

Questo reato è difficilmente commissibile nella realtà aziendale della Società.

Un modo possibile di realizzare il fatto di reato potrebbe essere il seguente.
Un dipendente della Società, responsabile della manutenzione e dello sviluppo delle infrastrutture informatiche per la gestione di pagamenti, desideroso di migliorare le performance del sistema di pagamento online della Società per ottenere riconoscimenti professionali, decide di integrare nel software un programma di terze parti che ha scoperto su un forum online.

Questo programma, oltre a snellire il flusso delle operazioni di pagamento, ha come funzione principale la generazione di numeri di carte di credito falsi per consentire transazioni fraudolente.

3. Area a rischio: "Gestione dei sistemi informativi aziendali e sicurezza dei dati"

3.1. Funzioni aziendali coinvolte

Le funzioni aziendali della Società coinvolte nell'attività di gestione dei sistemi informativi aziendali sono rappresentate dalle seguenti:

- Presidente del Consiglio di amministrazione
- Direttore generale;
- Area Servizi – Servizio Sistemi Informativi e Documentali;
- Area Amministrazione, Finanza, Pianificazione e Controllo di Gestione;
- Dipendenti di Romagna Acque assegnatari di strumenti hardware e software aziendali.
- Il Data Protection Officer incaricato

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. Procedure gestionali ed operative

Predisposte e mantenute aggiornate dall'Area Servizi, si riferiscono rispettivamente alle seguenti attività.

Il "*Regolamento Aziendale sul corretto utilizzo degli strumenti informatici*", fornisce un panorama completo sul corretto l'impiego sia delle apparecchiature hardware, che dei software in dotazione, in connessione anche al rispetto della normativa in materia di protezione dei dati personali e alla riduzione dei rischi connessi alle tecnologie informatiche.

Il documento "*Sistemi informativi – Descrizione generale*", che illustra il sistema informativo della Società in termini generali, con riferimento a tutte le aree aziendali, dalla telefonia, ai singoli strumenti informatici riguardanti l'amministrazione, il videocontrollo, il BIM (Building Information Modeling), ecc.

Il documento "*Servizio Sistemi Informativi e Telecomunicazioni – Organizzazione generale*", che descrive l'organizzazione del sistema IT, con definizione dell'organico, delle attività generali e delle interazioni, delle strategie e piani di lavoro, dei ruoli e compiti dei singoli componenti, ecc.

Un documento specifico, contenuto nel file "*SistInfo-DescrizioneTLCC.pdf*", riguardante la piattaforma di gestione dell'attività di conduzione e monitoraggio degli impianti e delle reti idriche, definito "Sistema informatizzato di telecomando e telecontrollo".Il documento "*SistInfo-TabellaEventiDisasterRecovery*", che, in riferimento ai sistemi informatici, riporta l'elenco dei possibili eventi di incidente, misure adottate, coinvolgimenti e tempi attesi di ripristino del servizio.Il documento "SistInfo-

IRP_istruzione operativa_RASF - Incident Respons plan". Descrive la pianificazione delle misure tecnologiche ed organizzative previste dall'azienda al fine di assicurare, in condizioni di emergenza, l'attuazione delle procedure necessarie per il ripristino dei sistemi informatici di elaborazione e gestione dei dati ed il ripristino dall'emergenza, con conseguente ripresa dell'erogazione dei servizi informatici ritenuti essenziali per li funzionamento dei processi aziendali

Il documento "SistInfo-ComunicazionePresaInCarico", che riporta la comunicazione di presa in carico strumentazione informatica da sottoscrivere da parte del dipendente.

Il documento "Regolamento videosorveglianza" : regolamento generale sull'utilizzo degli strumenti di videosorveglianza

Il documento "B7-4 Lettera Nomina Amministratore di Sistema": nomina ad Amministratore di Sistema ai sensi del Provvedimento del Garante Privacy del 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008), modificato in base al provvedimento del 25 giugno 2009

Il documento "B7-5 Lettera password": nomina ad incaricato, in relazione al sistema di videosorveglianza aziendale, ai fini dell'individuazione della password per l'accesso alle immagini registrate e per il trattamento dei dati personali e delle immagini connesse

Il documento "B7-6 Lettera visione diretta": nomina ad incaricato, in relazione al sistema di videosorveglianza aziendale, ai fini della visione in diretta delle immagini videoriprese e per il trattamento dei dati personali e delle immagini connesse.

Il documento "B7-7 Lettera immagini registrate" : nomina ad incaricato, in relazione al sistema di videosorveglianza aziendale, ai fini della visione delle immagini registrate e per il trattamento dei dati personali e delle immagini connesse.

Il "Regolamento per la messa a disposizione della rete in fibre ottiche agli operatori del settore Telecomunicazioni", approvato dal CdA.

Il "Regolamento per la messa a disposizione dei siti di Romagna Acque per l'ospitalità di impianti di operatori del settore Telecomunicazioni", approvato dal CdA

Agli specifici documenti sopra indicati, si affiancano i "*manuali operativi"*, documenti strutturati che raccolgono e descrivono in modo sistematico le prescrizioni necessarie per svolgere correttamente determinate attività, rappresentando una guida pratica e dettagliata che standardizza le modalità operative, garantendo uniformità e coerenza nell'esecuzione dei compiti.

Più che semplici raccolte di istruzioni, i manuali operativi sono veri e propri strumenti di gestione che supportano il controllo dei processi, la qualità del lavoro e l'efficienza organizzativa, fornendo un quadro di riferimento chiaro e condiviso per tutte le figure coinvolte nelle attività descritte.

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

Gestione dei sistemi informativi e sicurezza dati			
Area a rischio	**Flussi informativi**	**Periodicità**	***Key Officer***
Gestione dei sistemi informativi aziendali	Report avente ad oggetto l'attività svolta, con rilievo dei fatti che, a parere del Key Officer, sulla base della propria esperienza e dei documenti aziendali, possono costituire segnali di allarme prodromici alla violazione del Codice etico, del Codice di comportamento, del MOG e del PTPCT adottato. Dovrà comunque essere data evidenza minima dei seguenti punti. 1. eventuali incidenti IT verificatisi, cause, relativi processi di risposta attivati e risultati ottenuti; 2. eventuali interventi di modifica sui sistemi informativi realizzati, motivazioni e risultati ottenuti; 3. eventuali autorizzazioni all'installazione di software diversi da quelli messi a disposizione dalla Società rilasciate, motivazioni e risultati ottenuti;	**Semestrale**	**Responsabile della Funzione "Servizio Sistemi Informativi e Documentali"**

	4. controlli e verifiche periodiche sull'efficienza del sistema e risultati ottenuti, con particolare evidenza su scostamenti rispetto alle previsioni o standard di riferimento; 5. 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 verifica effettuata, rimedi, risultati ottenuti ed evidenze di applicazioni del sistema sanzionatorio; 6. 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; 7. 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; 8.		

Gestione dei dati sensibili *ex* D.lgs. n. 196/2003	Report avente ad oggetto l'attività svolta, con rilievo dei fatti che, a parere del Key Officer, sulla base della propria esperienza e dei documenti aziendali, possono costituire segnali di allarme prodromici alla violazione delle policy aziendali attinenti al rispetto della normativa sulla privacy. Dovranno comunque essere formalizzate le seguenti relazioni. ***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	**Semestrale**	**Responsabile della Funzione "Servizio Sistemi Informativi e Documentali"**
	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;	**Semestrale**	**Responsabile della Funzione "Servizio Sistemi Informativi e Documentali"**

INFORMAZIONI NON ORDINARIE			
Area	**Flussi informativi**	**Periodicità**	***Key Officer***
Generale	***Report* aventi ad oggetto (che dovranno essere riportati per sintesi nelle relazioni periodiche):** 1. eventuali non conformità e rimedi assunti relativi all'applicazione del flusso; 2. eventuali non conformità e rimedi assunti rispetto a prassi e procedure aziendali; 3. eventuali non conformità e rimedi assunti rispetto alle disposizioni del codice etico e del codice di comportamento; 4. eventuali non conformità e rimedi assunti rispetto al D.lgs. n. 231/2001 e al Modello 231 ed al PTPCT adottato; 5. eventuali deroghe alle procedure di processo decise in caso di emergenza o di impossibilità temporanea di attuazione, motivazioni e risultati relativi; 6. verifica rispondenza della rappresentatività delle procedure rispetto alle sequenze di azioni compiute in azienda; 7. eventuali utilizzi illegittimi, da parte del personale, delle attrezzature software e hardware ricevute in dotazione,	**Al riscontro della non conformità**	**Responsabile della Funzione "Servizio Sistemi Informativi e Documentali"**

	con esito della verifica effettuata, rimedi, risultati ottenuti ed evidenze di applicazioni del sistema sanzionatorio.		
Gestione delle attività relative alle telecomunicazioni	***Segnalazione delle 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.***	**Annuale**	**Responsabile Area Servizi-RASA**