



Modello di Organizzazione, Gestione e Controllo di ASM Codogno S.r.l. ai sensi del D.lgs. 231/2001

PROTOCOLLO DI DECISIONE 231 N.09

GESTIONE DEI SISTEMI INFORMATIVI

Approvato con delibera del Consiglio di Amministrazione in data 19/12/2024

INDICE

1. OBIETTIVO	2
2. AMBITO DI APPLICAZIONE	4
3. RUOLI COINVOLTI NELL'AREA DI RISCHIO	5
4. ATTIVITÀ RELATIVE ALL'AREA DI RISCHIO.....	5
5. PRINCIPI DI COMPORTAMENTO.....	6
6. PRINCIPI DI CONTROLLO	10
6.1. LIVELLI AUTORIZZATIVI.....	10
6.2 SEGREGAZIONE DELLE FUNZIONI AZIENDALI	11
6.3 PRINCIPI PROCEDURALI GENERALI	11
6.3.1 PRINCIPI PROCEDURALI SPECIFICI	13
6.4 TRACCIABILITÀ DEL PROCESSO DECISIONALE E ARCHIVIAZIONE	18
7. REPORTING ALL'ORGANISMO DI VIGILANZA	20
7.1 FLUSSI INFORMATIVI AD EVENTO	20
7.2 VIOLAZIONI DEL PROTOCOLLO DI PARTE SPECIALE (SEGNALAZIONI WHISTLEBLOWING).....	21
8. MODALITÀ DI GESTIONE DEL DOCUMENTO	21

1. Obiettivo

Il presente protocollo, che costituisce parte integrante del Modello di Organizzazione, Gestione e Controllo ex D.lgs. 231/2001 di **ASM Codogno S.r.l.** (di seguito anche “**ASM Codogno** “ o “Società”), ha l’obiettivo di definire i ruoli, le responsabilità, i principi di comportamento e di controllo che la Società intende osservare, con riferimento alle diverse attività relative all’area di rischio “**Gestione dei sistemi informativi**”, nel rispetto della normativa vigente e dei principi di trasparenza, oggettività e veridicità delle informazioni e con la finalità di prevenire, nell’esecuzione delle medesime attività, la commissione di illeciti previsti dal D.lgs. 231/2001.

In particolare, il presente documento, in conformità a quanto previsto dal suddetto decreto, intende prevenire il verificarsi della commissione, anche a titolo di concorso con altre funzioni aziendali e soggetti terzi, delle seguenti fattispecie di reato:

- **Reati informatici:**

- **Accesso abusivo a sistema informatico e telematico / detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici**, per esempio, accedendo senza autorizzazione ai sistemi informativi di terzi (es. enti concorrenti), protetti da misure di sicurezza (siano esse di tipo *hardware* o *software*) ovvero mantenendosi nei sistemi informativi di cui si abbiano le credenziali per motivi diversi da quelli per cui é stata concessa l'autorizzazione.
- **Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche / detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche**), per esempio, ove tali condotte siano realizzate, anche con il concorso di fornitori esterni, verso enti concorrenti, al fine di acquisire informazioni riservate o per interrompere la trasmissione di documentazione per la partecipazione ad una gara (concorrenza sleale).
- **Danneggiamento di informazioni, dati e programmi informatici**, per esempio, nel caso si proceda, con il concorso di fornitori esterni, a danneggiare sistemi informatici altrui (es. società concorrenti) o della documentazione ivi mantenuta, allo scopo di distruggere informazioni, dati o programmi, impedendone l'attività ed ottenendone un vantaggio competitivo, nell’interesse o a vantaggio.

Il reato può essere commesso anche in caso di danneggiamento di **informazioni, dati e programmi informatici, nonché sistemi informatici o telematici anche pubblici o di pubblico interesse.**

- **Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico**, per esempio, nel caso di diffusione tramite apparecchiature aziendali di programmi informatici (es. virus), autonomamente sviluppati o reperiti da fornitori esterni, con la finalità di danneggiare i sistemi informatici o telematici di enti concorrenti, pubblici o privati.
- **Estorsione informatica**, allorché, con il concorso di fornitori esterni, venga commesso o si minacci di commettere taluni reati informatici espressamente richiamati dalla norma (tra cui, l'accesso abusivo o l'intercettazione/interruzione di comunicazioni informatiche o la falsificazione/alterazione/soppressione del contenuto di comunicazioni informatiche o telematiche ovvero il danneggiamento di informazioni e sistemi informatici) al fine di costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno. A titolo di esempio, nell'interesse o a vantaggio della Società, tramite la diffusione di malware nei sistemi informatici di un soggetto terzo, si procede alla criptazione dei file al fine di richiedere un riscatto per renderli nuovamente intelleggibili.
- **Falsità in documenti informatici**, ad esempio nel caso in cui venga gestito il sistema documentale alterando documenti elettronici pubblici aventi efficacia probatoria (es. disposizioni bancarie, documenti word di vario genere, e-mail contenenti informazioni rilevanti, file di log, algoritmi di firma elettronica).
- **Delitti in materia di violazione del diritto d'autore:**
 - **Violazione della normativa in materia di diritto d'autore (in ambito ICT)** nel caso di installazione sui sistemi informatici aziendali di programmi in assenza dei necessari diritti di utilizzazione economica o di regolari licenze rilasciate dal titolare dei diritti d'autore (duplicazione abusiva di software).
 - **Abusiva riproduzione di una banca dati**, nel caso di duplicazione delle informazioni contenute in una banca dati in assenza dei necessari diritti di utilizzazione economica o di regolari licenze rilasciate dal titolare dei diritti d'autore.

- **Reati societari:**

- **False comunicazioni sociali**, allorché la Società esponga fatti materiali non rispondenti al vero oppure ometta fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale e finanziaria della società, in modo concretamente idoneo da indurre altri in errore, nell'interesse o vantaggio della Società (ad esempio, alterando i dati contenuti nel sistema informativo aziendale utilizzato per la gestione della contabilità).

- **Reati contro la Pubblica Amministrazione:**

- **Frode informatica commessa ai danni dello Stato**, ad esempio nell'ipotesi in cui la Società, anche con il concorso di terze persone, riesca ad alterare i registri informatici della Pubblica Amministrazione (i.e. Agenzia delle Entrate, INAIL, ecc.), per modificare dati fiscali/previdenziali/ecc. di interesse dell'azienda, già trasmessi all'Amministrazione.

Il processo in esame potrebbe altresì favorire la commissione del reato di **truffa ai danni dello Stato**, allorché la gestione fisica e logica della rete, dei dati informatici nonché dei backup non garantisca gli standard minimi di sicurezza (es. adozione di password di accesso alla rete, la segregazione delle cartelle, ecc.), permettendo un accesso indiscriminato ai dati informatici e ciò favorisca l'alterazione di informazioni, dati e file destinati agli Enti Pubblici. Tali falsificazioni potrebbero infatti costituire artifici o raggiri a danno della Pubblica Amministrazione, procurando contestualmente a ASM Codogno S.r.l. un ingiusto profitto (es. il rilascio di concessione/autorizzazione/rimborso/agevolazione non dovuta, o l'omissione di una sanzione).

2. Ambito di applicazione

Il presente protocollo si applica a tutti i Destinatari del Modello, ovvero ai dipendenti e dirigenti di ASM Codogno, ai componenti degli organi sociali e ai Soggetti Terzi¹, inclusi coloro i quali, pur non essendo funzionalmente legati alla Società ma agendo

¹ Quali, a titolo esemplificativo e non esaustivo, e così come definiti dal Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/01 della Società: i collaboratori a progetto, gli stagisti, i lavoratori interinali.

sotto la direzione o la vigilanza dei responsabili aziendali, sono coinvolti a qualsiasi titolo nelle attività relative all'area di rischio in oggetto.

Il presente protocollo richiama ed integra quanto già disciplinato nell'ambito del Codice Etico.

Si precisa che ogni qualvolta il presente protocollo richiama il Codice Etico, e in generale tutto il corpo procedurale applicato in ASM Codogno S.r.l., si fa riferimento, di volta in volta, alla versione più recente, vigente in un certo momento temporale.

ASM Codogno adeguerà il proprio comportamento a quanto esposto nel presente protocollo. Il mancato rispetto di quanto disposto nel presente protocollo da parte dei Destinatari è passibile di sanzioni disciplinari nei termini previsti dal Modello adottato dalla Società.

3. Ruoli coinvolti nell'area di rischio

Il processo di “Gestione dei sistemi informativi” di ASM Codogno S.r.l. prevede il coinvolgimento, secondo le rispettive competenze, dei seguenti soggetti:

- Presidente del CdA (Rappresentante dell'impresa)
- Responsabili delle aree di sviluppo software
- IT Support ²
- ogni dipendente e collaboratore (*user* ³)
- consulenti esterni (fornitori professionisti IT).

4. Attività relative all'Area di rischio

Le attività che rientrano nell'area di rischio “Gestione dei sistemi informativi”, ai fini dell'applicazione del presente protocollo, sono le seguenti:

- A. Gestione dei sistemi informativi, della qualità dei dati e dei servizi ICT;**
- B. Gestione della sicurezza delle informazioni e della compliance ICT;**
- C. Gestione dei cambiamenti IT e di sicurezza delle informazioni.**

Le modalità operative per la gestione delle diverse attività relative all'area di rischio in oggetto, laddove necessario, potranno essere disciplinate nell'ambito di appositi

² Si tratta di fornitore esterno.

³ Per “user” si intende ogni utilizzatore del sistema informativo aziendale.

regolamenti e procedure interne sviluppate ed aggiornate a cura a cura delle competenti Unità Operative.

5. Principi di comportamento

Il Sistema di Controllo interno ex d.lgs. 231/2001, per essere valutato efficace ed idoneo, deve garantire che tutte le Funzioni aziendali siano formate ed informate circa il corretto *modus operandi* nell'esecuzione di ogni attività di cui risultano essere destinatarie, circa i comportamenti da tenere e quelli espressamente vietati, la cui violazione potrebbe comportare l'avvio di un provvedimento disciplinare.

I Destinatari che, per ragione del proprio incarico o della propria funzione, sono coinvolti nelle attività relative all'area di rischio "*Gestione dei sistemi informativi*", sono tenuti ad osservare le previsioni di legge e i regolamenti esistenti in materia, le regole sancite dal presente Protocollo, nonché le norme etico – comportamentali adottate dalla Società.

In particolare, i Destinatari devono:

A. Per la Gestione dei sistemi informativi, della qualità dei dati e dei servizi ICT:

- rispettare i vincoli normativi e regolamentari applicabili in ragione dello specifico oggetto sociale e dell'attività economica che viene svolta dalla Società (es. L. 190/2012, D.Lgs. 33/2013, D.Lgs. 175/2016 e ss.mm.ii., e Linee Guida di ANAC applicabili);
- tenere un comportamento corretto e trasparente, assicurando un pieno rispetto delle norme di legge e regolamentari, nonché delle procedure della Società, nello svolgimento di tutte le attività;
- definire criteri per la selezione e la gestione del personale adibito al trattamento dei dati e allo svolgimento di operazioni critiche (amministratori di sistema e utenti privilegiati) con particolare riguardo alla valutazione delle competenze e dell'affidabilità del personale;
- in caso di modifica dell'operatività, aggiornare tempestivamente le procedure connesse;
- prevedere un adeguato piano formativo e informativo al personale circa l'utilizzo dei sistemi informativi e delle misure di sicurezza;

B. Per la Gestione della sicurezza delle informazioni e della compliance ICT:

- provvedere al mantenimento della sicurezza delle dotazioni informatiche aziendali e della riservatezza dei propri dati di accesso, al fine di evitare un utilizzo fraudolento o improprio delle stesse;
- adottare misure di attenuazione di tipo tecnico o organizzativo, idonee a contenere il “rischio informatico”;
- garantire che nello svolgimento delle operazioni critiche siano rispettati il principio del minimo privilegio e della segregazione dei compiti (ad es. procedure di abilitazione e di autenticazione);
- garantire l’accesso ai sistemi informativi aziendali tramite credenziali personali (l’utilizzo di password complesse e/o strong authentication per l’accesso ai sistemi/device);
- accedere alle aree dei sistemi informativi per i quali si è in possesso dei necessari profili di autorizzazione;
- utilizzare le risorse informatiche aziendali rispettando le misure di sicurezza stabilite dalla Società (modifica e custodia delle password, utilizzo dei sistemi di protezione quali antivirus, etc.) evitando comportamenti che possano comprometterne il loro corretto funzionamento o generare danni a terze parti;
- assicurare il rispetto delle norme interne, comunitarie e internazionali poste a tutela del software (programmi per elaboratore e banche dati), promuovendone un uso corretto;
- curare con diligenza gli adempimenti di carattere amministrativo necessari per l’utilizzo del software nell’ambito della gestione del sistema informativo aziendale;
- monitorare in modo costante l’operatività dei sistemi informatici e ogni user al fine di identificare prontamente eventuali incidenti informatici;
- segnalare alla Funzione IT/Ufficio preposto eventuali incidenti di sicurezza fornendo tutte le informazioni e l’eventuale documentazione necessari per una corretta valutazione del caso.

C. Per la Gestione del cambiamento IT e di sicurezza delle informazioni:

- qualora sia previsto il coinvolgimento di soggetti terzi/outsourcer nella gestione dei sistemi informatici e del patrimonio informativo della Società, i contratti devono imporre a tali fornitori il rispetto di idonee misure di sicurezza anche nell’ottica di prevenire la commissione di illeciti rilevanti che

possano comportare una responsabilità amministrativa ex d.lgs. 231/2001 per la Società;

- nel caso di sviluppi software affidati in appalto a società esterne, tutelarsi contrattualmente, anche ai fini della prevenzione della responsabilità amministrativa ex d.lgs. 231/2001, nei confronti dei fornitori rispetto a possibili violazioni del diritto d'autore e più in generale dei diritti di proprietà intellettuale da questi commesse quali, a titolo esemplificativo, utilizzo di software contraffatto e/o di codici sorgenti o parti di essi appartenenti a terzi in assenza delle necessarie autorizzazioni;
- adottare ogni misura organizzativa e tecnica al fine di ostacolare ogni indebito utilizzo o falsificazione di strumenti di pagamento (materiali o immateriali) diversi dal contante.

In ogni caso è **fatto divieto** di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del d.lgs. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- trascurare l'aggiornamento costante dell'organigramma ICT-IT nonché la definizione di ruoli e responsabilità del personale e delle misure tecnico-organizzative adottate per la sicurezza;
- omettere la revoca dei diritti e delle responsabilità e le rispettive autorizzazioni in caso di re-organizzazione interna o la modifica organizzativa;
- detenere, installare e utilizzare software (programmi) non approvati dalla Società e/o privi delle necessarie autorizzazioni/ licenze;
- realizzare qualunque condotta finalizzata, in generale, alla duplicazione, di programmi per elaboratore protetti o banche di dati sulla memoria fissa del computer;
- utilizzare i beni aziendali e, in particolare, le dotazioni informatiche aziendali, per commettere o indurre alla commissione di reati o per perseguire qualsiasi finalità contraria a norme di legge vigenti o che possa costituire una minaccia per l'ordine pubblico, la tutela dei diritti umani o il buon costume;
- alterare documenti informatici pubblici aventi efficacia probatoria e ogni altro documento in formato elettronico;
- accedere abusivamente ai sistemi informatici o telematici aziendali e/o di soggetti pubblici o privati (es. società concorrenti) anche al fine di acquisire illecitamente, alterare o cancellare dati e/o informazioni;

- procurarsi, detenere, riprodurre, diffondere, comunicare o consegnare codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornire indicazioni o istruzioni idonee al predetto scopo;
- procurarsi, detenere, produrre, riprodurre, importare, diffondere, comunicare, consegnare o, comunque, mettere a disposizione di altri apparecchiature, dispositivi o programmi informatici 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;
- intercettare fraudolentemente e/o impedire e/o interrompere comunicazioni relative a sistemi informatici o telematici e/o intercorrenti tra più sistemi;
- detenere, installare apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative sistemi informatici o telematici e/o intercorrenti tra più sistemi;
- detenere, diffondere, installare abusivamente programmi diretti a danneggiare o interrompere un sistema informatico;
- installare software non autorizzati, duplicare abusivamente software protetti da licenza, effettuare registrazioni o riproduzioni audiovisive, elettroniche, cartacee o fotografiche di documenti aziendali, salvo i casi in cui tali attività rientrino nel normale svolgimento delle funzioni affidate;
- formare falsamente ovvero alterare o sopprimere, anche parzialmente, il contenuto, anche occasionalmente intercettato, di comunicazioni relative a sistemi informatici o telematici e/o intercorrenti tra più sistemi;
- distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici altrui;
- commettere azioni dirette 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;
- distruggere, danneggiare, rendere, anche parzialmente, inservibili sistemi informatici o telematici altrui o ostacolarne gravemente il funzionamento attraverso condotte di danneggiamento o l'introduzione o la trasmissione di dati, informazioni o programmi;

- commettere azioni dirette a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, attraverso condotte di danneggiamento o l'introduzione o la trasmissione di dati, informazioni o programmi;
- accedere senza autorizzazione a sistemi informativi utilizzati dalla Pubblica Amministrazione o di alterarne, in qualsiasi modo, il funzionamento o di intervenire con qualsiasi modalità cui non si abbia diritto su dati, informazioni o programmi contenuti in un sistema informatico o telematico o a questo pertinenti per ottenere e/o modificare informazioni a vantaggio della Società, o comunque al fine di procurare un indebito vantaggio alla Società;
- falsificare documentazione da inoltrare alla Pubblica Amministrazione nell'interesse o a vantaggio della Società, e contestualmente cagionando danno allo Stato;
- realizzare qualunque condotta finalizzata, in generale, alla duplicazione di programmi per elaboratore protetti o banche di dati sulla memoria fissa del computer;
- alterare in qualsiasi modo il funzionamento di un sistema informatico o telematico intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi, se dal fatto si produce un trasferimento di denaro, di valore monetario o di valuta virtuale;
- alterare, falsificare o manomettere strumenti di pagamento diversi dal contante impiegati dalla Società;
- occultare o distruggere corrispondenza o ogni altra documentazione relativa al presente protocollo.

6. Principi di controllo

Il Sistema di Controllo a presidio delle attività in oggetto si deve basare su alcuni elementi qualificanti a garanzia dell'oggettività e trasparenza delle scelte effettuate, che tutti i Destinatari, che per ragione del proprio incarico o della propria funzione sono coinvolti nelle attività di approvvigionamento di beni e servizi e gestione degli incarichi a professionisti esterni, devono osservare.

6.1. LIVELLI AUTORIZZATIVI

Il Sistema di Controllo interno ex d.lgs. 231/2001, per essere valutato efficace e idoneo, deve prevedere l'esistenza di **specifici livelli autorizzativi**, definiti in modo chiaro e preciso a livello aziendale, tramite la predisposizione di un sistema di deleghe e procure specifico per il processo, nonché l'attribuzione dei poteri di rappresentanza e di firma sociale.

In particolare, occorre che:

- a) i poteri e le responsabilità siano chiaramente definiti e conosciuti all'interno dell'organizzazione;
- b) i poteri autorizzativi e di firma siano coerenti con le responsabilità organizzative assegnate e opportunamente documentati in modo da garantirne, all'occorrenza, un'agevole ricostruzione ex post;
- c) a nessuno vengano attribuiti poteri illimitati.

Il Sistema di Controllo interno al processo di "*Gestione dei sistemi informativi*" deve pertanto prevedere un **sistema di deleghe e procure** che coinvolge i vari Ruoli aziendali, informi il sistema di profilazione per l'accesso alla rete ed ai sistemi informativi.

6.2 SEGREGAZIONE DELLE FUNZIONI AZIENDALI

Il Sistema di Controllo interno ex d.lgs. 231/2001, per essere valutato idoneo ed efficace, deve garantire l'applicazione del **principio di segregazione delle funzioni aziendali**, mediante la suddivisione e la distribuzione dei poteri e delle responsabilità in capo ai diversi soggetti che intervengono, a vario titolo, nello stesso processo aziendale. In particolare, a nessuna Funzione aziendale si devono conferire poteri autonomi e svincolati da verifiche e controlli da parte di altre Funzioni.

Le procedure ed i regolamenti devono, in ogni caso, rispettare i vincoli normativi applicabili alla Società e derivanti, a titolo esemplificativo, dalla L. 190/2012 (Legge anticorruzione), dal D.Lgs. 33/2013 (Legge sulla Trasparenza nella Pubblica Amministrazione), dal D.Lgs. 175/2016 (Testo unico in materia di società a partecipazione pubblica), e ss.mm.ii., nonché di provvedimenti emanati dall'Autorità Nazionale Anticorruzione applicabili.

Tutte le procedure ed i regolamenti, adottati da ASM Codogno per la "*Gestione dei sistemi informativi*", devono pertanto rispettare il **principio di separazione dei compiti** fra le funzioni coinvolte nelle attività autorizzative, esecutive e di controllo.

6.3 PRINCIPI PROCEDURALI GENERALI

Il Sistema di Controllo interno ex d.lgs. 231/2001, per essere valutato efficace ed idoneo, deve prevedere **specifiche procedure e regolamenti** e deve garantire che tutte le Funzioni aziendali siano formate ed informate circa il corretto *modus operandi* nell'esecuzione di ogni attività di cui risultano essere destinatarie. Le procedure ed i regolamenti devono altresì evidenziare i comportamenti da tenere e quelli espressamente vietati, la cui violazione potrebbe comportare l'avvio di un provvedimento disciplinare.

Tutte le procedure ed i regolamenti adottati da ASM Codogno, relativi all'area di rischio "*Gestione dei sistemi informativi*", devono pertanto rispettare i seguenti **principi procedurali generali**, in grado di garantire il corretto funzionamento dell'organizzazione aziendale ed evitare il verificarsi di condotte criminose, prevedendo:

A. la previsione di controlli specifici e peculiari per le singole attività che compongono un processo aziendale, quali presidi contro la commissione di condotte che costituiscono reato.

Il Sistema di Controllo interno ex d.lgs. 231/2001, per essere valutato efficace ed idoneo, deve chiaramente indicare **tutti i presidi a controllo del rischio** di commissione reato.

A titolo meramente esemplificativo, nella gestione del processo di "*Gestione dei sistemi informativi*", si deve prevedere:

- un sistema di profilazione e di segregazione per l'accesso alla rete ed ai sistemi informativi, allineato al sistema di deleghe e procure;
- criteri e modalità di esecuzione dei *backup* dei dati presenti sui sistemi informativi e sui PC aziendali;
- criteri di complessità nella scelta delle *password* per accedere alla rete.

B. la tracciabilità delle operazioni compiute all'interno del processo, che garantisce la correttezza e completezza del processo stesso, nonché l'integrità di tutto l'iter autorizzativo.

Il Sistema di Controllo interno ex d.lgs. 231/2001, per essere valutato efficace ed idoneo, deve prevedere che, per ogni operazione, vi debba essere un adeguato supporto documentale su cui si possa procedere, in ogni momento, all'effettuazione di controlli che attestino le caratteristiche e le motivazioni dell'operazione e individuino chi ha autorizzato, effettuato, registrato, verificato l'operazione stessa.

In ottemperanza al **principio di trasparenza**, ogni attività deve essere tracciata in modo chiaro, corretto, completo, per consentire la ricostruzione delle responsabilità, delle motivazioni delle scelte operate e delle fonti informative.

Nella gestione del processo il Sistema di Controllo deve pertanto prevedere la conservazione e l'archiviazione della documentazione afferente all'iter di gestione dei sistemi informativi e dei diritti d'autore in ambito ICT, che deve necessariamente comprendere:

- la formalizzazione della comunicazione della richiesta di attivazione dei profili di accesso alla rete aziendale e ai sistemi informativi e relativa autorizzazione;
- la conservazione del regolamento relativo al corretto utilizzo, da parte dei dipendenti, dei PC/device aziendali e dei relativi sistemi informativi;
- l'elenco degli incidenti informativi verificatisi;
- la conservazione dei supporti di *backup*.

La Società deve altresì conservare l'evidenza documentale di ogni eventuale operazione compiuta in deroga alla procedura, e della relativa giustificazione.

6.3.1 PRINCIPI PROCEDURALI SPECIFICI

La Società nella predisposizione delle procedure e dei regolamenti che disciplinano le attività afferenti al processo di “*Gestione dei sistemi informativi*”, rivolge particolare attenzione all'esigenza di garantire il rispetto dei seguenti **principi procedurali specifici**, prevedendo:

A. Per la fase “GESTIONE DEI SISTEMI INFORMATIVI, DELLA QUALITÀ DEI DATI E DEI SERVIZI ICT”

- la definizione ed il costante aggiornamento dei ruoli e responsabilità del personale in ambito ICT-IT;
- la definizione delle misure tecniche e organizzative di base adottate per garantire presidi adeguati di gestione dei sistemi informativi e la mitigazione dei rischi operativi;
- durante le re-organizzazioni interne o le cessazioni dei rapporti di lavoro o la modifica anche temporanea della mansione, la revoca dei diritti e delle responsabilità e le rispettive autorizzazioni;
- la previsione di un adeguato piano di formazione e informazione circa le tecnologie e controlli IT su cui opera il personale;
- la definizione e formalizzazione dell'architettura aziendale ICT- IT che consenta la visione dei componenti IT (hardware e software) aziendali e delle loro interazioni;

- la previsione di un time-out di sessione quando l'utente non è attivo per un determinato periodo di tempo;
- la progettazione, realizzazione e manutenzione dei presidi di sicurezza dei data center;
- la definizione e la formalizzazione dei criteri e delle modalità di esecuzione dei backup dei dati presenti sui sistemi informativi e sui PC aziendali;
- l'adozione di un sistema che consenta l'esecuzione di un backup periodico (in relazione al sistema informativo) automatico dei dati presenti sui sistemi informativi e sui PC aziendali secondo i criteri e le modalità stabilite dalla Società, anche da parte degli outsourcer;
- l'invio delle richieste di assistenza tecnica e/o richiesta di servizio da parte della risorsa (user) ad un soggetto qualificato e con opportune conoscenze in ambito ICT-IT;
- la valutazione delle richieste/segnalazioni ricevute da parte di soggetto qualificato e con opportune conoscenze in ambito ICT-IT;
- in caso di incidenti, la definizione di procedure dettagliate per garantire una risposta efficace e ordinata agli incidenti informatici;
- l'ingaggio di soggetti competenti in materia di *information technology*, per la risoluzione delle problematiche rilevate;
- la tempestiva e adeguata protezione dei file di log da manomissioni e accessi non autorizzati;
- la verifica della produzione di un log di distruzione dei documenti;
- il presidio costante, in capo alla risorsa all'uopo delegata della modifica o dell'aggiornamento dei dati, eseguito dai fornitori dei sistemi informativi, durante il loro ciclo di vita o una volta già archiviati;
- la previsione dell'impossibilità per gli utenti di disporre di privilegi per installare o disattivare applicazioni software non autorizzate;
- l'adozione di misure idonee ad evitare che vengano rimossi arbitrariamente o elusivamente i dispositivi applicati per proteggere i programmi tutelati da licenza d'uso;
- la previsione dell'aggiornamento periodico dei software installati;
- lo svolgimento di controlli periodici atti a verificare i software installati sui computer.

B. Per la fase “GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI E DELLA COMPLIANCE ICT”

- la predisposizione e l'adozione e la diffusione di un documento relativo alla modalità di corretto utilizzo, da parte dei dipendenti, dei PC/device aziendali, dei relativi sistemi informativi, di internet e della posta elettronica;
- la definizione di disposizioni atte a garantire la sicurezza fisica dei dati, attraverso la regolamentazione degli accessi ai locali contenenti i server aziendali e le modalità di accesso;
- la previsione delle misure di sicurezza dei locali contenenti i server aziendali (quali, l'uso di chiavi di accesso ai locali o badge, il registro degli accessi, l'installazione di un gruppo di continuità, sistema di condizionamento, ingressi separati, sistema antincendio, porta taglia fuoco, pavimento galleggiante ecc.);
- la definizione di disposizioni atte a garantire la sicurezza logica dei dati, attraverso la regolamentazione degli accessi e le modalità di accesso alla rete e ai sistemi/applicativi IT;
- la predisposizione di meccanismi di segregazione (ad esempio tramite l'utilizzo di directory e l'assegnazione di privilegi adeguati al personale), al fine di regolamentare l'accesso alle cartelle di rete presenti nella rete aziendale;
- l'integrazione dell'analisi dei rischi informatici nell'ambito della gestione dei rischi operativi dell'organizzazione;
- la definizione di una politica di controllo degli accessi che stabilisca le regole di controllo di accesso appropriate, i diritti di accesso e le restrizioni per ruoli utente specifici verso i processi aziendali;
- la definizione, sulle applicazioni aziendali, dei corretti ruoli in relazione alle mansioni attribuite nell'ambito dei processi in cui il personale è coinvolto, assicurando il rispetto del criterio dei minimi privilegi necessari connessi con le necessità lavorative;
- l'aggiornamento tempestivo delle procedure o policy per la sicurezza informatica, da parte di Soggetto competente in materia di information security;

- l'assegnazione a ciascun ruolo aziendale di specifici diritti di accesso alla rete, agli applicativi, in ottemperanza al sistema di deleghe e procure previsto dalla Società e sulla base delle effettive esigenze operative (principio della stretta pertinenza e necessità);
- l'utilizzo di un sistema informatico in grado di differenziare e limitare gli accessi da parte degli utenti (user) nel rispetto di privilegi assegnati;
- l'assegnazione di accessi privilegiati solo a membri specifici dell'organizzazione;
- la definizione delle misure tecniche e organizzative di base adottate per garantire la protezione dei sistemi informativi e delle informazioni gestite;
- la definizione di clausole contrattuali con il fornitore di servizi o sistemi IT-ICT che specifichino i requisiti e gli obblighi concordati per il rispetto delle politiche di sicurezza e l'attuazione delle misure di protezione delle informazioni dell'organizzazione;
- la previsione della disattivazione e/o cancellazione delle credenziali di autenticazione al sistema informativo aziendale, nel caso di cessazione del rapporto di lavoro o prolungata assenza di accesso;
- lo svolgimento di una verifica, con cadenza periodica, della sussistenza delle condizioni per la conservazione dei profili di autorizzazione di accesso alla rete;
- l'assegnazione di un codice identificativo dell'utente (user-id) associato ad una componente segreta di autenticazione (parola chiave o password), per l'accesso ai sistemi informativi/device aziendali;
- la previsione dell'autenticazione a due fattori per accedere a determinati sistemi informatici aziendali o ai device mobili (i fattori di autenticazione potrebbero essere password, token di sicurezza, chiavette USB con un token segreto, biometria ecc.);
- la previsione dell'obbligo di modifica (automatizzata) delle credenziali di autenticazione al sistema informatico;
- l'esecuzione tempestiva dell'analisi del rischio informatico, al verificarsi di situazioni in grado di influenzare il complessivo livello di rischio informatico;
- la previsione dell'impossibilità per gli utenti di disattivare o aggirare le impostazioni di sicurezza (sicurezza workstation);

- la previsione della protezione fisica dei dispositivi mobili contro il furto quando non sono in uso;
- la previsione della tempestiva installazione degli aggiornamenti di sicurezza critici rilasciati dallo sviluppatore del sistema operativo;
- l'adozione di sistemi/strumenti informatici, quali software antivirus e antimalware, su tutte le macchine, volti a ridurre il rischio di perdita o sottrazione delle informazioni in formato elettronico;
- la conservazione (per una durata predefinita) della versione aggiornata dei back up, presso un ambiente protetto e coerente con gli standard applicati sui dati originari;
- la verifica del regolare svolgimento delle attività di backup dei sistemi informativi;
- la conservazione di una copia aggiornata dei backup in modalità off-line, assicurando misure di sicurezza fisica paragonabile a quelle previste per i sistemi in produzione, e modalità di conservazione idonee a garantire l'integrità dei supporti e dei dati ivi contenuti;
- la conservazione di un elenco degli incidenti informatici gravi verificatisi;
- l'esecuzione di un'attività di analisi degli incidenti gravi allo scopo di definire le possibili azioni di miglioramento per evitare il ripetersi dell'incidente e/o migliorare la capacità di reazione dell'organizzazione;
- la registrazione delle azioni degli amministratori di sistema e degli operatori di sistema, tra cui aggiunta/cancellazione/modifica dei diritti utente;
- la sincronizzazione temporale dei dati di log (gli orologi vengono sincronizzati con un'unica sorgente di tempo di riferimento, es. NTP server);
- la previsione dell'impossibilità di cancellazione o modifica del contenuto dei file di log (l'accesso ai file di log deve inoltre essere registrato per consentire di rilevare l'attività insolita);
- la previsione che un sistema di monitoraggio elabori i file di log, produca report sullo stato del sistema e notifichi eventuali anomalie;
- la previsione dell'impossibilità per gli utenti di disporre di privilegi per installare o disattivare applicazioni software non autorizzate;
- la previsione dell'aggiornamento periodico dei software installati;

C. Per la fase “GESTIONE DEI CAMBIAMENTI IT E DI SICUREZZA DELLE INFORMAZIONI”

- la valutazione dell’impatto dei cambiamenti sul sistema e dei rischi correlati con le proposte di modifica;
- l’indicazione, da parte della Società ai propri fornitori, di direttive per la sicurezza fisica e per la gestione del rischio informatico;
- la definizione di clausole contrattuali con il fornitore di servizi o sistemi IT-ICT che specifichino i requisiti e gli obblighi concordati per il rispetto della politica di governo dei sistemi informativi e dei controlli atti ad assicurare una qualità idonea dei dati e dei servizi gestiti;
- la definizione di clausole contrattuali con il fornitore di servizi o sistemi IT-ICT che obbligano al rispetto della normativa del diritto d'autore (in ambito IT);
- l’esecuzione dell’analisi di conformità dei contratti di outsourcing e con fornitori;
- la tracciabilità di ogni comunicazione intercorsa tra Fornitori IT e le singole risorse interne;
- l'esecuzione di un controllo che tutte le modifiche apportate al sistema informativo siano registrate e monitorate da una persona specifica competente in materia di information technology;
- la tracciabilità degli accessi ai sistemi informativi e rilevazione delle eventuali anomalie circa la frequenza, la modalità e la temporalità di accesso;
- la definizione dei sistemi/applicazioni per i quali devono essere attivati i file di log e quali tipi di accesso deve essere incluso (vista, modifica, cancellazione dei dati);

6.4 TRACCIABILITÀ DEL PROCESSO DECISIONALE E ARCHIVIAZIONE

A garanzia del principio di trasparenza delle singole fasi del processo, al fine di consentire la ricostruzione delle responsabilità, delle motivazioni delle scelte e delle fonti informative, è prevista la tracciabilità del processo decisionale attraverso:

- la conservazione di:
 - supporti di *backup*;

- log di accesso raccolti;
- documentazione relativa sia alla sicurezza dei sistemi informativi che alla manifestazione di esigenze di implementazione di nuove funzionalità;
- licenze d'uso di applicativi e/o altri software particolari installati sui PC/device aziendali;
- documentazione relativa alla sicurezza fisica e logica della rete aziendale;
- elenco dell'hardware e del software distribuito;
- documento relativo alle modalità di corretto utilizzo, da parte dei dipendenti, dei PC/device aziendali, dei relativi sistemi informativi, di internet e della posta elettronica;
- elenco delle violazioni alle procedure e regolamenti in materia di sicurezza informatica;
- richieste di abilitazione all'accesso ai sistemi informatici, e relativa autorizzazione;
- elenco degli incidenti informatici verificatisi;
- lettere di nomina degli incaricati del trattamento e degli amministratori di sistema interni ed esterni, con definizione degli ambiti di autorizzazione;
- la tracciabilità di:
 - accessi ai sistemi informativi e rilevazione delle eventuali anomalie circa la frequenza, la modalità e la temporalità di accesso;
 - analisi dei rischi periodiche volte ad evidenziare le criticità dei sistemi e le misure da adottare per preservarne l'integrità in base alle esigenze aziendali, nel rispetto degli obblighi stabiliti dalle normative vigenti (es. Regolamento UE 679/2017, d.lgs.196/2003 e ss. mod., nonché i provvedimenti generali del Garante per la protezione dei dati personali);
 - controllo periodico del corretto funzionamento dei sistemi di protezione previsti dalla Società e destinati a garantire la sicurezza fisica e logica dei dati;
 - comunicazione della richiesta di attivazione dei profili di accesso alla rete aziendale e ai sistemi informativi e relativa autorizzazione da parte del Soggetto munito di idonei poteri;
 - verifica della sussistenza delle condizioni per la conservazione dei profili di autorizzazione di accesso alla rete e ai sistemi informativi;
 - richieste di assistenza tecnica e/o richiesta di servizio da parte della risorsa (user);

- comunicazioni intercorse tra il Fornitore di servizi in ambito tecnologico e le Funzioni interne, lettere di nomina degli incaricati del trattamento e degli amministratori di sistema interni ed esterni, con definizione degli ambiti di autorizzazione e dei log di accesso e delle operazioni sui dati, da parte dei Fornitori in ottemperanza della normativa vigente.

I Destinatari interessati sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente Protocollo 231.

7. Reporting all'Organismo di Vigilanza

Come previsto dal sistema dei flussi informativi verso l'Organismo di Vigilanza disciplinato nel Modello 231, qualora si verificano circostanze non espressamente regolamentate dal presente protocollo, che si prestino a dubbie interpretazioni e/o applicazioni o tali da imporre deroghe all'applicazione del protocollo medesimo, è fatto obbligo a ciascun Destinatario coinvolto di comunicare tempestivamente il verificarsi anche di una sola delle suddette circostanze al proprio diretto responsabile che, di concerto con l'OdV e il Responsabile di Funzione interessata, valuterà gli idonei provvedimenti in relazione alla singola fattispecie.

7.1 FLUSSI INFORMATIVI AD EVENTO

I Destinatari, direttamente o tramite il proprio Responsabile gerarchico, dovranno comunicare senza indugio all'Organismo di Vigilanza i seguenti flussi informativi:

- eventuali verifiche ed accertamenti da parte delle autorità preposte in materia di tutela dei dati personali;
- le violazioni (accertate internamente o ad opera di autorità competenti) relative ad adempimenti richiesti dalle normative vigenti in materia di protezione dei dati personali e di sicurezza informatica;
- eventuali gravi criticità emerse a seguito di verifiche, attività di audit o di controllo, effettuate internamente o con l'ausilio di soggetti esterni;
- l'aggiornamento di parti rilevanti delle policy e procedure in materia di sicurezza informatica;
- il verificarsi di gravi incidenti al sistema informativo aziendale, le ragioni degli stessi e le eventuali attività di controllo poste in essere;



- i risultati delle verifiche effettuate sul software installato sui sistemi e sugli apparati elettronici della Società.

I flussi informativi ad evento sopra elencati dovranno essere inviati all'OdV all'indirizzo di posta elettronica dedicato.

7.2 VIOLAZIONI DEL PROTOCOLLO DI PARTE SPECIALE (SEGNALAZIONI WHISTLEBLOWING)

Si ricorda che é responsabilità di tutti i Destinatari del Modello coinvolti nello svolgimento delle attività dell'area a rischio di segnalare tempestivamente, con le modalità previste dalla Procedura per la gestione delle segnalazioni whistleblowing, ogni informazione relativa a comportamenti costituenti violazione del presente Protocollo o relativi alla commissione di reati riconducibili al d.lgs. 231/2001.

8. Modalità di gestione del documento

Il presente documento é approvato dal Consiglio di Amministrazione.

Ogni modifica al documento deve essere preventivamente sottoposta all'Organismo di Vigilanza che ne valuterà l'adeguatezza e la coerenza rispetto al Modello della Società, prima dell'approvazione formale dello stesso da parte del Consiglio di Amministrazione.