

PROCEDURA 9 GESTIONE DELLE ATTIVITA' INFORMATICHE

INDICE:

1. OBIETTIVI
2. DESTINATARI E PROCESSI AZIENDALI COINVOLTI
3. DOCUMENTAZIONE INTEGRATIVA
4. PROTOCOLLI DI PREVENZIONE
 - a) *protezione dei dati*
 - b) *gestione delle postazioni informatiche*
 - c) *utilizzo delle risorse informatiche*
 - d) *predisposizione o utilizzo di documenti informatici pubblici aventi efficacia probatoria*
5. DISPOSIZIONI FINALI

1. Obiettivi¹

La presente procedura ha l'obiettivo di definire ruoli e responsabilità, nonché dettare protocolli di prevenzione al fine di prevenire il verificarsi delle fattispecie di reato previste nei seguenti articoli del D.lgs. 231/01 (a titolo riassuntivo, rimandandosi per l'analisi dettagliata all'appendice normativa di parte speciale del presente MOG231):

- art. 640 ter c.p. – frode informatica (art. 24 D.lgs. 231/01);
- delitti informatici e trattamento illecito di dati (art. 24 bis D.lgs. 231/01);
- delitti in materia di violazione del diritto d'autore (art. 25 novies d.lgs. 231/01)

La presente procedura è altresì volta a prevenire il reato di cui all'art. 416 c.p. (associazione per delinquere), laddove finalizzato alla commissione dei reati di cui sopra.

2. Destinatari e Processi aziendali previsti

La presente procedura trova applicazione nei confronti di tutti coloro che, nell'esercizio dell'attività di propria competenza a favore della Società, utilizzano i sistemi informatici e/o telematici della società.

¹ La presente procedura costituisce altresì misura integrativa per la prevenzione della corruzione, secondo quanto previsto dalla Mappatura dei rischi (allegata al Piano triennale di prevenzione della corruzione e della trasparenza 2023 - 2025).

I reati di c.d. “criminalità informatica” (quali quelli in precedenza indicati) prevedono quale presupposto la disponibilità di uno strumento informatico (pc, laptop, tablet, smartphone etc.) e la concreta disponibilità di accesso alle postazioni di lavoro.

Pertanto, i Destinatari della presente procedura vanno individuati in tutti coloro che utilizzano uno strumento informatico e/o hanno accesso alla posta elettronica e/o utilizzano programmi informatici e/o hanno accesso ad Internet.

3. Documentazione integrativa

La presente procedura richiama ed integra quanto già disciplinato nell’ambito della seguente documentazione:

- Statuto
- Sistema di governance
- Codice Etico
- Procedura Segnalazioni *Whistleblowing*
- Contratto di service
- Piano triennale di prevenzione della corruzione e della trasparenza 2023 - 2025
- Procedure del Sistema di Gestione, con particolare – ma non esclusivo – riferimento a PO.AS.04.1 - Gestione dei servizi di staff,
- Procedure del Sistema di Gestione Integrato, in applicazione delle regole previste per le attività di service con la Società API S.p.A. con particolare – ma non esclusivo – riferimento a:
 - PO.04.3 - Utilizzo infrastrutture informatiche aziendali
- Istruzione tecnica IT - Regolamento PEC_ – “*Regolamento Gestione PEC*”
- Altre procedure del presente MOG 231 cui si rinvia, per quanto di competenza, con particolare – ma non esclusivo – riferimento a:
 - procedura 1 (gestione dei rapporti con l’OdV) per quanto attiene ai flussi informativi e alle segnalazioni *whistleblowing*;
 - procedura 3 (gestione degli affidamenti di lavori, servizi e forniture) per quanto attiene agli acquisti di programmi informatici nonché di banche dati;
 - procedura 5 (gestione della proprietà intellettuale) per quanto attiene alla tutela della proprietà intellettuale;
 - procedura 7 (Anticorruzione e Gestione dei Rapporti con le PP.AA. e i Privati) per quanto attiene alla presentazione di documenti di gara telematici;
 - procedura 13 (gestione dei rapporti di service) per quanto attiene i servizi informatici di cui la società usufruisce in forza del contratto di service.

4. Protocolli di prevenzione

Si precisa che la società ha contrattualmente demandato ad API svolge una serie di servizi come da contratto agli atti della società, cui si rimanda nella sua formulazione attuale e nelle sue eventuali successive modifiche (di cui l’OdV deve essere tempestivamente informato), tra i quali:



| | | |
|--------------|--|--|
| 13.12.2024 | MODELLO DI ORGANIZZAZIONE E GESTIONE EX D.LGS. 231/01 | |
| REV. 2024/00 | Pag. 3 di 5 | PARTE SPECIALE PROCEDURA 2.9 ATTIVITA' INFORMATICHE |

- i servizi informatici.

Al fine di consentire un efficace controllo sui rapporti di service, ASST adotta MOG231 specularmente a quello di API, agevolando la confrontabilità e l'omogeneità delle procedure.

API, nello svolgimento dei suddetti servizi a favore di ASST, è tenuta a rispettare la speculare procedura 9 (Gestione delle postazioni informatiche) del proprio MOG231, unitamente agli ulteriori presidi previsti nel presente MOG 231.

I rapporti di service tra ASST e API sono regolati nell'apposita procedura (proc. 13) del presente MOG 231, cui si fa rinvio.

La Società rispetta e pretende il rispetto della normativa nazionale e sovranazionale vigente in materia di utilizzo degli strumenti informatici, sicurezza della rete e sicurezza fisica, privacy, copyright, anche in conformità a quanto stabilito nel Codice Etico, nelle istruzioni e procedure operative interne, nonché mediante attività di sensibilizzazione rivolte a tutti i lavoratori sul tema della pirateria informatica e delle relative conseguenze

La Società condanna qualunque comportamento volto ad alterare in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenire senza diritto e con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, al fine di procurare alla Società o ad altri un ingiusto profitto con altrui danno.

Ciascun Destinatario deve utilizzare lo strumento informatico messo a disposizione dalla Società per il solo espletamento della propria mansione.

Nello specifico, occorre conformarsi a quanto segue:

a) protezione dei dati

La Società adotta misure tecniche ed organizzative adeguate volte ad attuare in maniera efficace i principi di protezione dei dati a tutela di dipendenti e terzi, assicurando che:

- la raccolta dei dati personali avvenga per finalità determinate esplicite e legittime,
- il trattamento dei dati personali avvenga in modo lecito, corretto e trasparente, nonché in maniera da garantire un'adeguata sicurezza ed evitare trattamenti non autorizzati o illeciti, nonché la perdita, la distruzione o il danno accidentale,
- la conservazione dei dati personali avvenga in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati, nel rispetto della normativa di settore.

b) gestione delle postazioni informatiche

È fatto obbligo di:

- catalogare tutte le macchine presenti come previsto nella procedura di gestione della proprietà intellettuale (Proc. 5) del presente MOG231;

- garantire l'installazione di programmi informatici originali come previsto nella procedura di gestione della proprietà intellettuale (Proc. 5) del presente MOG231;
- impedire il download di programmi informatici non autorizzati e regolarmente licenziati come previsto nella procedura di gestione della proprietà intellettuale (Proc. 5) del presente MOG231;
- verificare la sicurezza della rete internet aziendale e la sicurezza fisica delle postazioni informatiche;
- limitare l'accesso ai siti internet non necessari per lo svolgimento dell'attività lavorativa, mediante formazione e informazione dei Destinatari e strumenti informatici;
- introdurre protezioni in grado di limitare l'accesso ai siti internet contenenti materiale pedopornografico;
- dotare ogni postazione informatica di password personalizzata abbinata allo username dell'utente e predisporre un sistema di registrazione di ogni accesso, garantendo l'aggiornamento periodico delle password dei singoli utenti;
- dotare ogni postazione informatica abilitata all'accesso ad internet ovvero alla posta elettronica aziendale di password personalizzata abbinata allo username e predisporre un sistema di registrazione di ogni accesso, garantendo l'aggiornamento periodico delle password dei singoli utenti;
- dotare ogni postazione informatica di meccanismi di stand-by protetti da password abbinata a username, al fine di evitare l'utilizzo indebito della macchina in caso di allontanamento temporaneo dell'utente;
- modificare le password periodicamente, come previsto dalla normativa di settore; ogni Destinatario è tenuto a custodire la propria password in modo da evitarne la divulgazione;

c) utilizzo delle risorse informatiche

A seguito dell'entrata in vigore, in data 5.04.2008, della Legge 18 marzo 2008 n. 48, attuativa della Convenzione del Consiglio d'Europa in tema di criminalità informatica, ai fini della prevenzione dei reati così introdotti ai sensi del D.lgs. 231/2001, in uno con quanto dettato sopra, è fatto divieto di:

- porre in essere condotte miranti all'accesso abusivo ad un sistema informatico o telematico altrui protetto da misure di sicurezza;
- effettuare download illegali di dati e informazioni aziendali altrui;
- utilizzare – nello svolgimento della propria mansione – dati e informazioni aziendali altrui ottenuti in modo illecito;
- detenere e diffondere abusivamente codici di accesso a sistemi informatici o telematici altrui protetti da misure di sicurezza;
- porre in essere condotte volte a danneggiare illecitamente informazioni, dati, programmi e sistemi informatici e telematici altrui;
- porre in essere condotte volte a intercettare fraudolentemente e diffondere comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi.

Inoltre, è vietato:

- accedere ad una postazione informatica aziendale con uno username e password diversi da quelli assegnati;
- porre in essere condotte che possano mettere a rischio l'integrità del sistema informatico aziendale;
- porre in essere condotte volte a superare le protezioni informatiche predisposte dalla Società;
- installare programmi informatici diversi da quelli autorizzati dalla Società.

d) predisposizione e/o utilizzo di documenti informatici pubblici aventi efficacia probatoria

Nel caso di predisposizione e/o uso di documenti informatici pubblici aventi efficacia probatoria, occorre:

- verificare la provenienza e la veridicità del documento informatico e del suo contenuto;
- conservare il documento e la relativa documentazione probante la veridicità del suo contenuto e la sua provenienza per il tempo prescritto dalla normativa di settore;
- arrestare il procedimento di predisposizione, utilizzo o invio allorquando la provenienza e/o la veridicità del documento o del suo contenuto siano dubbi, nonché informare senza indugio l'AU. L'OdV deve essere informato a mezzo di apposito report (*Report 2.1.1 – Report Flussi informativi verso l'OdV* ovvero mediante altra forma scritta comunque idonea).

È fatto divieto di proseguire nell'operazione sino alla verifica e successiva autorizzazione da parte dell'AU.

5. Disposizioni finali

Tutti i Destinatari hanno la responsabilità di osservare e far osservare il contenuto della presente procedura.

Fermo quanto previsto dalla procedura di Gestione dei Rapporti con l'OdV (Proc. 1), ciascun Destinatario è tenuto a comunicare/segnalare tempestivamente ogni anomalia/violazione di quanto previsto dalla presente procedura a mezzo degli appositi canali previsti nella Procedura di Gestione dei Rapporti con l'OdV (proc. 1) e nel sistema adottato ai sensi della Legge 190/2012.

La violazione della presente procedura e dei suoi obblighi di comunicazione e segnalazione costituisce violazione del MOG231 e illecito disciplinare passibile di sanzione ai sensi di legge e del CCNL applicabile.