PROCEDURA 9
GESTIONE DELLE
ATTIVITA' INFORMATICHE

INDICE:

1. OBIETTIVI
2. DESTINATARI
3. PROCESSI AZIENDALI COINVOLTI
4. PROTOCOLLI DI PREVENZIONE
    - 4.1. DOCUMENTAZIONE INTEGRATIVA
    - 4.2. PROCEDURE DA APPLICARE
    - 4.2.1. ALTRI PRESIDI DI CONTROLLO:
    - 4.2.2. GESTIONE DI ACCESSI ACCOUNT E PROFILI;
    - 4.2.3. GESTIONE DELLE RETI DI COMUNICAZIONI;
    - 4.2.4. GESTIONE DEI SISTEMI HARDWARE;
    - 4.2.5. GESTIONE DEI SISTEMI SOFTWARE;
    - 4.2.6. GESTIONE DEGLI ACCESSI FISICI AI SITI OVE SONO COLLOCATE LE INFRASTRUTTURE IT;
        - *a)* 4.2.7. PREDISPOSIZIONE O UTILIZZO DI DOCUMENTI INFORMATICI PUBBLICI AVENTI EFFICACIA PROBATORIA
5. ATTIVITÀ DELL'ODV
6. DISPOSIZIONI FINALI

1. Obiettivi

La presente procedura ha l'obiettivo di definire ruoli e responsabilità, nonché dettare protocolli di prevenzione e controllo, in relazione alla Gestione delle Attività Informatiche al fine di prevenire, nell'esecuzione di tale attività, la commissione degli illeciti previsti dal D.lgs. 231/2001.

In particolare, la presente procedura intende prevenire il verificarsi delle fattispecie di reato previste nei seguenti articoli del D.lgs. 231/01 (a titolo riassuntivo, rimandandosi per l'analisi dettagliata alla parte speciale del presente MOG 231):

- Documenti informatici (art. 491 *bis* c.p.);
- Accesso abusivo ad un sistema informatico o telematico (art. 615 *ter* c.p.);
- Detenzione, e diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615 *quater* c.p.);
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 *quater* c.p.);

- 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.);
- Estorsione (art. 629, comma 3, c.p.);
- Danneggiamento di informazioni, dati e programmi informatici (art. 635 *bis* c.p.);
- 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.);
- Danneggiamento di sistemi informatici o telematici (art. 635 *quater* c.p.);
- 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.);
- Danneggiamento di sistemi informatici o telematici di pubblico interesse (art. 635 *quinquies* c.p.);
- Violazione delle norme in materia di perimetro di sicurezza nazionale cibernetica (art. 1, comma 11, D.L. 21 settembre 2019, n. 105.).
- art. 640 ter c.p. – frode informatica (art. 24 D.lgs. 231/01)
- delitti in materia di violazione del diritto d'autore (art. 25 *novies* D.lgs. 231/01);
- delitti in materia di strumento di pagamento diversi dai contanti e trasferimento fraudolento di valori (art. 25 *octies*, 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

La presente Parte Speciale si riferisce a comportamenti posti in essere da amministratori, sindaci, dirigenti e dipendenti di ASP Asti, nonché collaboratori esterni, partnes, fornitori come già definiti della Parte Generale, ed in tutti coloro che utilizzano un personal computer e/o hanno accesso alla posta elettronica e/o utilizzano programmi informatici e/o hanno accesso ad internet (qui di seguito, tutti definiti "Destinatari").

Obiettivo della presente Parte Speciale è che tutti i Destinatari, come sopra individuati, adottino regole di condotta conformi a quanto prescritto della stessa al fine di impedire il verificarsi dei reati previsti nel Decreto.

3. Processi aziendali coinvolti

I Destinatari della presente procedura, per quanto rileva ai fini della prevenzione dei reati pocanzi menzionati, partecipano alla gestione delle attività informatiche principalmente (ed a titolo esemplificativo) attraverso i seguenti processi aziendali:

- ordinaria e straordinaria amministrazione

- coordinamento e gestione delle attività aziendali
- gestione dei sistemi informativi
- gestione della procedura espropriativa
- gestione dei dati personali
- svolgimento dei processi che richiedono l'utilizzo dello strumento informatico (gestione del profilo utente e del processo di autenticazione, gestione e protezione della postazione di lavoro, gestione degli accessi verso l'esterno, gestione e protezione delle reti sicurezza fisica dei sistemi informatici).

4. Protocolli di prevenzione

Ogni attività svolta con l'ausilio del mezzo informatico deve avvenire nel rispetto della normativa vigente, della normativa in materia di diritto d'autore, copyright e privacy, nonché nel rispetto di tutta la normativa nazionale ed internazionale concernente l'utilizzo dei mezzi informatici.

La società adotta misure tecniche ed organizzative adeguate volte ad attuare in maniera efficace i principi di protezione dei dati.

La presente Parte Speciale prevede espressamente a carico dei Destinatari, in via diretta o tramite apposite clausole contrattuali, i seguenti **obblighi**:

- osservare attentamente tutte le leggi, regolamenti e procedure vigenti, con particolare riferimento a quelle che disciplinano le attività IT;
- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali, in tutte le attività che coinvolgono sistemi informatici e telematici dell'azienda, di terzi e/o pubblici;
- tenere comportamenti corretti, nel rispetto delle norme di legge e delle procedure aziendali, ponendo la massima attenzione ed accuratezza nell'acquisizione, elaborazione ed illustrazione dei dati e delle informazioni elaborati;
- utilizzare i Sistemi Informatici aziendali e l'accesso ad internet ai siti consentiti, mediante il normale software di navigazione in rete in dotazione, solo per scopi leciti e legati all'attività lavorativa tali da non pregiudicare il patrimonio informativo aziendale e nel rispetto delle disposizioni normative tempo per tempo vigenti e delle disposizioni del Modello;
- utilizzare i certificati elettronici, di firma digitale con chiave pubblica o di meccanismi di crittografia dei dati per comunicazioni critiche, unicamente ai soggetti a tal fine espressamente autorizzati dalla Società e secondo le modalità indicate dalla Società.

La presente Parte Speciale prevede espressamente dei Destinatari – in via diretta o tramite apposite clausole contrattuali – i seguenti divieti:

- porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (art. 25-bis del Decreto);
- porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarle o favorirne la commissione;

- eludere od omettere le attività di controllo implementate dalla Società;
- acquisire abusivamente informazioni contenute nei sistemi informativi di terzi;
- danneggiare o interrompere un sistema informatico o telematico di terzi, pubblici o privati, nonché abusivamente procurarsi, detenere, produrre, riprodurre, importare, diffondere, comunicare, consegnare, mettere in altro modo a disposizione di altri o installare apparecchiature, dispositivi o programmi informatici diretti a danneggiare od interrompere un sistema informatico o telematico;
- porre in essere qualunque attività che possa determinare il danneggiamento, la distruzione, l'alterazione o la soppressione di informazioni, dati e programmi informatici di terzi, siano essi pubblici o privati;
- utilizzare abusivamente codici d'accesso a sistemi informatici e telematici nonché procedere alla diffusione degli stessi;
- cedere a Terzi, anche solo temporaneamente, qualsivoglia apparecchiatura informatica o telematica aziendale, nonché i relativi software, credenziali di accesso, oppure lasciare incustodite dette apparecchiature in luoghi accessibili a terzi fuori dai locali aziendali o rivelare le proprie o le altrui credenziali di autenticazione alla rete informatica;
- modificare le configurazioni dei software ed hardware aziendali o modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, …);
- accedere alla rete aziendale, ai programmi ed alle banche dati, siano essi aziendali o di terzi, con credenziali di accesso diverse da quelle assegnate;
- aggirare le regole di sicurezza imposte sugli strumenti informatici aziendali e sulle reti di collegamento interne ed esterne;
- eludere sistemi di controllo posti a presidio di sistemi informatici o telematici, e comunque di accedere ai predetti sistemi in mancanza delle necessarie autorizzazioni;
- porre in essere qualunque attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni informatiche o telematiche, nonché procurarsi, detenere, produrre, riprodurre, diffondere, importare, comunicare, consegnare, mettere in altro modo a disposizione di altri o installare apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche, fuori dai casi consentiti dalla legge;
- installare o utilizzare strumenti software e/o hardware che potrebbero essere adoperati per valutare o compromettere la sicurezza di sistemi informatici o telematici (es. sistemi per individuare le password, decifrare i file criptati, …);
- procurarsi, produrre, riprodurre, diffondere, importare, comunicare, consegnare, mettere in altro modo a disposizione di altri o installare 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 fornire indicazioni o istruzioni idonee al predetto scopo;
- utilizzare computer, reti o altri dispositivi digitali per minacciare, manipolare o costringere qualcuno a fare o ad omettere qualcosa (a titolo esemplificativo e non esaustivo attraverso l'invio di e-mail di phishing, o l'impiego di altre forme di malware), ottenendo un ingiusto profitto e causando danno ad

– altri;

- mascherare, oscurare o sostituire la propria identità e inviare e-mail riportanti false generalità o inviare intenzionalmente e-mail contenenti virus o altri programmi in grado di danneggiare o intercettare dati;
- porre in essere condotte dirette alla distruzione o alterazione di documenti informatici aventi finalità probatoria qualora tale comportamento non rientri espressamente in procedure aziendali o sia dettato da motivazioni di tipo tecnico o funzionale;
- fornire informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi o delle attività ispettive di vigilanza ovvero omettere le relative comunicazioni in violazione di quanto previsto dal D.L. 21 settembre 2019, n. 105.

L'uso dei supporti informatici, della posta elettronica, dei programmi informatici, della rete internet deve avvenire conformemente nel rispetto di quanto previsto nelle procedure del Sistema Gestione Qualità, integralmente richiamata per quanto di competenza.

4.1. Documentazione integrativa

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

- Statuto
- Codice Etico
- Poteri deleghe e procure
- Processo di Incident Management
- Piano di Gestione delle segnalazioni
- Direttiva NIS2 (Network and Information Security 2)

  Allegato 4: Incidenti significativi di base per i soggetti essenziali
- LA TASSONOMIA CYBER DELL'ACN: definizione della tassonomia cyber dell'Agenzia per la cybersicurezza nazionale
- ISO/IEC/ 27035
- Documento per la pianificazione e gestione in materia di prevenzione del malaffare ex L. 190/2012 e trasparenzaMisure Integrative per la prevenzione della corruzione
- Manuale del Sistema di Gestione Integrato per la Qualità e l'Ambiente
- Sistema di Gestione per la Qualità, con particolare - ma non esclusivo - riferimento alla procedura "*Gestione sistemi informativi"*
- Disciplinare Interno ASP – Email e Internet in ufficio
- 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 i flussi informativi e le segnalazioni verso l'OdV;

- procedura 5 (gestione dei rapporti di industria e commercio) per quanto attiene il rapporto con le altre imprese;
- procedura 10 (gestione dei rapporti consulenziali) per quanto attiene la gestione del rapporto con il consulente informatico;
- procedura 14 (tutela del dipendente che segnala irregolarità e possibili episodi di corruzione (c.d. Whistleblowing) per quanto attiene le segnalazioni all'RPCT;

4.2. Procedure da applicare

4.2.1. Altri presidi di controllo

Gli obiettivi fondamentali che la Società si pone nella gestione del sistema informatico sono i seguenti:

a. riservatezza: garanzia che un determinato dato sia preservato da accessi impropri e sia utilizzato esclusivamente dai soggetti autorizzati. Le informazioni riservate devono essere protette sia nella fase di trasmissione, sia nella fase di memorizzazione/conservazione, in modo tale che l'informazione sia accessibile esclusivamente a coloro che sono autorizzati a conoscerla;
b. integrità: garanzia che ogni dato della Società sia realmente quello originariamente immesso nel sistema informatico e sia stato modificato esclusivamente in modo legittimo. Si deve garantire che le informazioni vengano trattate in modo tale che non possano essere manomesse o modificate da soggetti non autorizzati;
c. disponibilità: garanzia di reperibilità di dati inerenti all'attività della Società in funzione delle esigenze di continuità dei processi e nel rispetto delle norme che ne impongono la conservazione storica.

Ai fini della prevenzione dei reati di cui al D.lgs. 231/01, occorre segnatamente:

4.2.2. Gestione di accessi, account e profili

La designazione delle credenziali di autorizzazione (username, password, smart card ecc.) per i collaboratori o dipendenti chiamati ad utilizzare strumenti informatici aziendali deve avvenire in base a procedure sicure e che prevedano il loro periodico aggiornamento;

L'amministratore del sistema conserva e, in base a strette procedure, può accedere, all'elenco delle abilitazioni concesse. Periodicamente gli accessi concessi (intesi come numero di utenze abilitate) devono essere riverificati per valutare quali mantenere attivi e quali disabilitare.

Il conferimento delle credenziali di accesso al sistema informatico aziendale deve avvenire nei limiti in cui ciò sia funzionale allo svolgimento degli incarichi a ciascuno assegnati. A tal fine ogni utente è dotato di id e password che gli consentono (da qualsiasi postazione) di accedere soltanto alle informazioni cui egli è stato abilitato.

L'utilizzo delle password, dei codici di accesso, delle smart card personali, nonché l'utilizzo e la conservazione di qualunque altro dato o informazione utili a consentire l'accesso in un sistema informatico o telematico di ASP Asti o di terzi, deve avvenire nel rispetto rigoroso delle procedure e delle autorizzazioni previste per ciascuno.

È vietata la memorizzazione, l'acquisizione o l'invio di username, password, PIN, PUK ecc., da parte dei soggetti diversi dagli amministratori di sistema a ciò espressamente autorizzati.

Le credenziali di autorizzazione (username, password, smart card ecc.) devono essere mantenute segrete, costituiscono beni aziendali da non cedere o trasmettere a nessuno e da salvaguardare in ogni modo.

È fatto assoluto divieto di accedere alla rete aziendale o ai programmi con codici di identificazioni di altri utenti.

Ogni ipotesi o sospetto di intrusione o accesso abusivo al sistema aziendale o dal sistema aziendale, deve essere comunicato immediatamente al superiore gerarchico e al Responsabile dei Sistemi Informativi;

4.2.3. Gestione delle reti di comunicazioni

Deve essere garantito che l'accesso al sistema informatico interno (intranet) ed esterno (internet) avvenga nell'esercizio delle mansioni e per le finalità assegnate a ciascun utente;

deve essere vietata la connessione (e conseguenti consultazione, navigazione, downloading di dati o programmi) con riferimento a siti web contrari all'etica aziendale, che presentino contenuti illeciti, contrari alla morale, all'ordine pubblico, che consentano la violazione della privacy, riconducibili ad attività di pirateria informatica, che violino diritti d'autore, ecc.

L'accesso a sistemi informatici e banche dati di proprietà di terzi (specialmente se di pubblica utilità) può avvenire solo ove consti il consenso espresso o tacito dei proprietari, deve avvenire senza aggiramento o violazione dei dispositivi di sicurezza eventualmente predisposti e, in caso di restrizioni all'accesso, può avvenire solo da parte dei soggetti che abbiano preventivamente ottenuto l'autorizzazione degli amministratori del sistema.

L'utilizzo della posta elettronica deve avvenire per esigenza di servizio, con divieto di trasmettere attraverso tale strumento credenziali di autorizzazione personali proprie o di terzi, mail contenenti programmi non sicuri o illeciti (virus, spyware, ecc.), mail dirette a impedire o rallentare la funzionalità di sistemi informatici, ecc.; è altresì generalmente vietato utilizzare lo strumento della posta elettronica come mezzo per consentire la divulgazione all'esterno non autorizzata di dati aziendali mediante il meccanismo dei file allegati.

Deve essere garantito che gli utenti aziendali accedano alle risorse informatiche dall'esterno o dall'interno, solo attraverso specifici canali ragionevolmente sicuri.

4.2.4 Gestione dei sistemi hardware

Il compito di provvedere alle esigenze informatiche della Società curando l'investimento in componenti hardware nonché la definizione e gestione del loro corretto funzionamento è affidata al Responsabile dei Sistemi Informativi.

La manutenzione del sistema hardware (verifica fisica, integrità del sistema, scanning memorie, assenza di dispositivi di disturbo, assenza di alterazioni non autorizzate ecc.) è affidata al Responsabile dei Sistemi Informativi; tutti i server e le postazioni di lavoro sono protetti da programmi antivirus, regolarmente aggiornati;

Gli utenti devono curare il corretto utilizzo dei personal computers di pertinenza, non lasciarli incustoditi o sbloccati senza screensaver. Particolare attenzione deve essere prestata nella custodia e nell'uso dei dispositivi portatili.

È fatto divieto di installare componenti hardware non debitamente autorizzati o comunque non funzionali al corretto utilizzo dei sistemi informatici e telematici di ASP Asti o di terzi.

I supporti rimovibili, prima del loro riutilizzo (es. in caso di licenziamento dell'addetto o sostituzione delle risorse informatiche assegnate) devono essere messi in sicurezza attraverso idonee procedure di formattazione.

4.2.5 Gestione dei sistemi software

È fatto divieto di utilizzare o installare programmi diversi da quelli autorizzati dalla Società.

È sempre e comunque vietato installare programmi diretti alla commissione di illeciti quali distruzione di dati, intercettazioni, manomissioni di archivi, interruzioni di comunicazioni ecc.

L'utilizzo ovvero la modifica a vario titolo dei software forniti dall'azienda devono avvenire solo se autorizzati e secondo le istruzioni operative ricevute.

Il downloading deve essere strettamente regolamentato e limitato ai programmi sicuri e di libero accesso.

Ogni singolo utente è responsabile del salvataggio e memorizzazione dei dati che gestisce e deve curarne la sicurezza ed integrità.

Sono previsti:

• BACKUP giornalieri – conservati per [●] giorni successivi al salvataggio;

• BACKUP settimanali – conservati per [●] giorni successivi al salvataggio;

• BACKUP mensili – conservati per un [●] successivo al salvataggio;

• BACKUP annuali – nessuna scadenza.

Le policy aziendali vietano l'installazione di software non autorizzato per mantenere l'integrità dei sistemi.

Qualsiasi tentativo di installare software non autorizzato viene bloccato e segnalato.

La Società non effettua controlli sui dispositivi per verificare che i software installati siano regolarmente licenziati.

4.2.6. Gestione degli accessi fisici ai siti ove sono collocate le infrastrutture IT

I dispositivi telematici, i server, i supporti di salvataggio dei backup sono collocati in aree dedicate, protetti da armadi muniti di serratura accessibili al solo personale autorizzato.

Non è consentito l'accesso alle aree riservate (quali server rooms, locali tecnici, ecc.) alle persone che non dispongono di idonea autorizzazione temporanea o permanente e, in ogni caso, nel rispetto della normativa vigente in materia di tutela dei dati personali;

La sicurezza fisica dell'infrastruttura tecnologica della azienda deve essere curata nel rispetto della normativa sulla sicurezza nei luoghi di lavoro.

Altre regole finalizzate alla prevenzione dei reati informatici in genere.

Al fine di garantire un maggior controllo sui sistemi informatici e sulle attività ad essi collegate, il servizio IT di ASP Asti ha progressivamente reingegnerizzato i propri processi interni introducendo

quindi il CISO quale responsabile della sicurezza delle informazioni e dei sistemi informatici. Rientra in tale pratica il processo di Incident Management.

4.2.7. Protezione dei sistemi informatici o telematici da eventuali danneggiamenti

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, occorre:

- individuare le persone fisiche abilitate all'accesso al server aziendale;
- individuare le persone fisiche abilitate all'accesso ai sistemi informatici e alle banche dati nel rispetto della normativa in materia di trattamento dei dati personali;
- esplicitare i sistemi informatici e telematici e le relative banche dati accessibili, vietando l'accesso a quelli non espressamente indicati;
- esplicitare i limiti di azione delle persone suddette all'interno dei sistemi telematici e delle banche dati, predisponendo misure tecniche ed organizzative adeguate volte ad attuare in maniera efficace i principi di protezione dei dati;

4.2.8. Predisposizione o utilizzo di documenti informatici pubblici aventi efficacia probatoria

Nel caso di predisposizione o uso di documenti informatici qualificabili come atto pubblico, copia autentica e/o attestato, occorre:

- verificare la provenienza e la veridicità del documento e del suo contenuto;
- conservare il documento cartaceo e la relativa documentazione cartacea probante la veridicità del suo contenuto e la sua provenienza nel fascicolo di competenza (da costituirsi necessariamente all'atto della predisposizione o dell'utilizzo di un documento informatico di cui sopra qualora esso non faccia parte di un fascicolo già esistente – ad esempio archivio fatture);
- arrestare il procedimento di predisposizione, utilizzo o invio allorquando la provenienza e/o la veridicità del documento o del suo contenuto siano dubbi, nonché informarne senza indugio le competenti autorità aziendali e l'RPCT mediante gli appositi canali previsti nella "Procedura per la tutela del dipendente che segnala irregolarità e possibili episodi di corruzione (c.d. Whistleblowing) (proc. 14). È fatto divieto di proseguire nell'operazione in assenza di autorizzazione dell'AD.

5. Attività dell'ODV

Premessi i generali poteri di iniziativa e controllo, l'OdV ha facoltà di:

- prendere visione di tutti i documenti concernenti la gestione delle postazioni informatiche;
- accedere ai documenti telematici inviati, al fine di verificare la loro coincidenza con gli atti originali cartacei ovvero con i dati sulla base dei quali è stato predisposto il documento telematico;

- verificare la corrispondenza tra i programmi dichiarati come installati sul PC e quelli effettivamente presenti;
- verificare le licenze dei programmi installati sui PC.

L'OdV incontra (se nominato) il Responsabile della Protezione dei Dati (RDP/DPO) almeno una volta all'anno, nonché ogni volta ciò si renda necessario.

In tali incontri, l'OdV è facoltizzato a richiedere tutte le informazioni ritenute necessarie per verificare la corretta applicazione di quanto previsto nella presente procedura.

6. Disposizioni finali

Tutte le funzioni aziendali coinvolte 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 all' RPCT ogni anomalia/violazione di quanto previsto dalla presente procedura mediante gli appositi canali previsti nella *"Procedura per la tutela del dipendente che segnala irregolarità e possibili episodi di corruzione*" (c.d. Whistleblowing) (proc. 14)

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 contratto collettivo nazionale di lavoro applicabile.