

REGOLAMENTO INFORMATICO

Allegato C al Modello di organizzazione, gestione e controllo
ai sensi del decreto legislativo 8 Giugno 2001 n° 231

Approvato dal CdA di PROVIDENTIA S.R.L. in data 30/03/2016

Versione 2 del 30/03/2016

Sommario

1. PREMESSA.....	3
2. ACCESSO AL SISTEMA INFORMATIVO AZIENDALE	3
3. UTILIZZO DEL PERSONAL COMPUTER.....	4
4. GESTIONE DELLE PASSWORD.....	5
5. UTILIZZO DEI SUPPORTI MAGNETICI.....	6
6. USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI.....	6
6.1 Accesso Fortinet Vodafone Rete Unica Diretta (MPLS di VRUD).....	7
7. UTILIZZO DI PC PORTATILI.....	7
8. USO DELLA POSTA ELETTRONICA.....	7
8.1. Disponibilità dei messaggi di posta elettronica.....	8
9. ATTIVITÀ DI VERIFICA.....	9
10. CESSAZIONE DEL RAPPORTO DI LAVORO.....	9
11. SANZIONI PER INOSSERVANZA DELLE NORME.....	9
12. AGGIORNAMENTO E REVISIONE	10

1. PREMESSA

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai personal computer nonché l'accesso e l'utilizzo per scopi lavorativi di banche dati esterne, se da una parte è diventata essenziale per l'operatività aziendale, espone dall'altra a rischi di un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza ed all'immagine dell'Azienda stessa.

In questo senso, viene fortemente sentita dai datori di lavoro la necessità di porre in essere adeguati sistemi di controllo sull'utilizzo di tali strumenti da parte dei dipendenti e di sanzionare conseguentemente quegli usi scorretti che, oltre ad esporre l'azienda stessa a rischi tanto patrimoniali quanto penali, possono di per sé considerarsi contrari ai doveri di diligenza e fedeltà previsti dagli artt.2104 e 2105 del codice civile.

I controlli preventivi e continui sull'uso degli strumenti informatici devono garantire tanto il diritto del datore di lavoro di proteggere la propria organizzazione, essendo i computer aziendali strumenti di lavoro la cui utilizzazione personale è preclusa, quanto il diritto del lavoratore a non vedere invasa la propria sfera personale, e quindi il diritto alla riservatezza ed alla dignità come sanciti dallo Statuto dei lavoratori e dal D.lgs 196/03 sulla tutela dei dati personali.

LA VILLA S.P.A. ha adottato quindi il presente Regolamento Informatico, allegato al Modello di Organizzazione, gestione e controllo redatto ai sensi del D.Lgs 231/2001, che costituisce policy per l'intero Gruppo Societario, diretto ad evitare che comportamenti, anche inconsapevoli, possano innescare rischi di commissione di reati o minacce alla sicurezza nel trattamento dei dati.

Il presente documento, adottato dal CdA di LA VILLA SPA, si estende dunque a tutte le Società del Gruppo, che dovranno recepirlo formalmente all'interno del proprio Modello di Organizzazione, gestione e controllo.

In ragione di quanto sopra, ogni richiamo nel presente documento a LA VILLA S.P.A., o LA VILLA, o Azienda/Società, dovrà intendersi esteso a tutte le Società del Gruppo, controllate da LA VILLA S.P.A.

Detto Regolamento è stato approvato dal CDA di Providentia srl il 30 marzo 2016.

In particolare si ricorda a tutti i dipendenti che il D.Lgs 231/2001 prevede specifici reati:

- in materia informatica che fanno capo all'art. 24-bis del D.Lgs 231/2001 "Delitti informatici e trattamento illecito di dati";
- in materia di diritto d'autore che fanno capo all'art. 25 novies "Reati in materia di violazione del diritto di autore";
- in materia di pornografia che fanno capo all'art. 25 quinquies "Delitti contro la personalità individuale".

Tali reati vengono sono descritti nell'Allegato E del Modello di organizzazione, gestione e controllo adottato dall'azienda.

2. ACCESSO AL SISTEMA INFORMATIVO AZIENDALE

All'atto dell'assunzione ogni dipendente PROVIDENTIA S.R.L., riceve gli strumenti di lavoro essenziali per svolgere la propria mansione e, tra questi, può essere previsto l'uso di personal computer, di apparati telefonici, smartphone/tablet con accesso alla rete internet ed alla posta elettronica.

Il *Responsabile Sistema Informatico* aziendale è responsabile di fornire al dipendente gli strumenti informatici (registrandone l'assegnazione) e le necessarie informazioni per il corretto accesso alle risorse informatiche aziendali.

Per ciascun dipendente (o gruppi di dipendenti) deve essere eseguita un'adeguata profilazione che tenga conto delle mansioni da svolgere, degli applicativi da utilizzare e delle risorse informatiche alle quali accedere (es. stampanti, cartelle di rete, etc.).

Per il primo accesso al sistema viene fornita dal *Responsabile Sistema Informatico* al dipendente una id personale ed una password temporanea, che il dipendente avrà compito di modificare tempestivamente, secondo le indicazioni successive (par. 4).

Ulteriori specifici account (Id utente e password) possono essere forniti sempre dal *Responsabile Sistema Informatico* aziendale per l'accesso a siti e banche dati esterne, laddove previsto in base alla mansione svolta.

Ogni assegnazione al dipendente di account per l'accesso a risorse informatiche aziendali o esterne, deve essere registrata (ed aggiornata nel tempo) a cura del *Responsabile Sistema Informatico* aziendale.

E' dato incarico a tutti i responsabili aziendali di comunicare tempestivamente eventuali cambi di mansione che comportino modifiche o revoche di autorizzazione all'accesso delle risorse informatiche, sia all'ufficio del personale che al *Responsabile Sistema Informatico* (che in PROVIDENTIA assume anche il ruolo di Amministratore di Sistema previsto dalla normativa privacy), per iscritto, al fine di rendere possibili le modifiche dei profili di accesso alle risorse e la sostituzione delle password ove necessario.

Il *Responsabile Sistema Informatico* è inoltre responsabile di fornire eventuali accessi temporanei al sistema informativo aziendale per dipendenti, collaboratori o soggetti esterni all'organizzazione, laddove questi siano stati autorizzati da parte della Direzione aziendale o da Responsabili di Area.

Stesse modalità devono essere seguite per l'utilizzo delle risorse informatiche aziendali (es. reti wi-fi) per l'accesso alla rete internet tramite computer, notebook, smartphone, tablet da parte di personale esterno.

3. UTILIZZO DEL PERSONAL COMPUTER

Il Personal Computer affidato al dipendente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

Si dispone pertanto che tutto il personale usi la massima cura nella gestione delle apparecchiature informatiche di cui è responsabile e si attenga rigorosamente alle seguenti disposizioni:

1. Le apparecchiature informatiche devono essere utilizzate solo per scopi aziendali e non privati;
2. Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione esplicita del *Responsabile Sistema Informatico*, in quanto sussiste il grave pericolo di violare specifiche leggi in materia di diritto d'autore nonché di importare Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore; in particolare, installando programmi cosiddetti "di rete" senza le necessarie verifiche di compatibilità, è possibile compromettere il funzionamento del server, dei database ivi contenuti e/o della rete stessa.

Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal *Responsabile Sistema Informatico* di PROVIDENTIA

L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'azienda a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (D. Lgs. 518/92

sulla tutela giuridica del software, L. 633/1941 Legge sul diritto d'autore, L. 248/2000 nuove norme di tutela del diritto d'autore) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore; in merito si precisa che anche il software freeware spesso è tale solo per uso personale e non aziendale e pertanto soggetto a licenza d'acquisto.

3. I Personal Computer e i loro componenti (stampanti, casse, CD software etc.) devono essere custoditi con cura unitamente alla documentazione con cui originariamente sono stati consegnati;
4. La postazione di lavoro e le relative periferiche, quali stampanti locali e di rete, scanner, etc., devono essere spente al termine dell'attività lavorativa o in caso di assenze prolungate dall'ufficio. Eventuali eccezioni dovranno essere formalmente autorizzate dal Responsabile IT. Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso; pertanto l'utente, ogni qualvolta si allontani dalla propria postazione, deve procedere al blocco della macchina mediante la pressione contemporanea dei tasti CTRL+ALT+CANC seguita da INVIO. Il ripristino della stessa avverrà soltanto attraverso l'immissione della password di accesso a client;
5. Gli utenti autorizzati ad accedere alla rete pubblica internet possono farlo solo per scopi legati alla normale attività aziendale e per esigenze di ufficio;
6. E' assolutamente vietato scaricare da Internet dati, immagini, video e/o programmi non strettamente correlati all'attività lavorativa;
7. E' cura degli utilizzatori provvedere alla archiviazione periodica dei dati (non dei programmi): si sottolinea che i dati sono di proprietà aziendale e non personale e che la perdita degli stessi può causare grave danno all'Azienda la cui responsabilità ricade sull'utilizzatore;
8. Non è consentito all'utente modificare le caratteristiche di sistema (nome computer, indirizzi IP, DNS, Firewall, aggiornamenti automatici SW, etc.) preimpostate sul proprio PC, salvo previa autorizzazione esplicita del *Responsabile Sistema Informatico*;
9. Non è consentito connettere alla rete aziendale Personal Computer aziendali o di terzi in maniera autonoma non autorizzata dal *Responsabile Sistema Informatico*; l'inosservanza di tale norma può essere causa di gravi rischi alla sicurezza e alla funzionalità aziendale;
10. Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, cellulari, lettori mp3, etc.), se non con l'autorizzazione espressa del *Responsabile Sistema Informatico*;
11. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il *Responsabile Sistema Informatico* nel caso in cui vengano rilevati virus.

4. GESTIONE DELLE PASSWORD

Si dispone che l'accesso ai computer, ai programmi (applicativi) o ad eventuali banche dati esterne avvenga solo attraverso l'utilizzo di parole chiavi riservate, le password.

Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; devono essere composte da almeno otto caratteri e non devono contenere riferimenti agevolmente riconducibili all'incaricato. In particolare, si raccomanda di usare, preferibilmente, nella composizione della password almeno un carattere numerico,

uno maiuscolo e uno speciale e non basarla su informazioni facilmente deducibili, quali il proprio nome, il nome dei famigliari, la data di nascita, il codice fiscale e simili.

Di seguito alcune regole di gestione delle password personali:

- non permettere ad altri utenti (es. colleghi) di operare con il proprio identificativo utente;
- non trascrivere la password su supporti (es. fogli, post-it) facilmente accessibili a terzi;
- non utilizzare le cosiddette "password di gruppo", ovvero generalizzate per area o mansioni di appartenenza, neanche qualora siano Responsabili d'area/struttura o Direttori a richiederlo. A questa regola generale può derogarsi solo, per condizioni particolari e specifiche, dietro autorizzazione del *Responsabile del sistema informatico* previa analisi dei rischi correlati all'utilizzo dei dati.

La segretezza delle password utilizzate deve essere custodita dall'incaricato con la massima diligenza e non divulgata.

La password deve essere immediatamente sostituita, dandone comunicazione al Custode delle Parole chiave, identificato nel *Responsabile Sistema Informatico*, nel caso si sospetti che la stessa abbia perso la segretezza.

Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia alla Direzione o persona dalla stessa incaricata (*Responsabile del sistema informatico*).

È necessario procedere alla modifica della password a cura dell'utente del sistema al primo utilizzo e, successivamente, almeno ogni sei mesi; nel caso di trattamento di dati sensibili e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi (come previsto dal punto 5 del disciplinare tecnico allegato al Codice della privacy, D.Lgs n. 196/2003).

Non è consentita l'attivazione della password firmware di accensione (bios-setup), senza preventiva autorizzazione da parte del *Responsabile Sistema Informatico*, il quale agisce come Amministratore di sistema.

5. UTILIZZO DEI SUPPORTI MAGNETICI

Tutti i supporti magnetici riutilizzabili (dischetti, DVD, penne USB, cassette, cartucce) contenenti dati sensibili e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.

I supporti magnetici contenenti dati sensibili e giudiziari devono essere custoditi in archivi chiusi a chiave.

6. USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

Il computer abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa.

È pertanto assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal *Responsabile Sistema Informatico*.

È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla Direzione (Presidente CdA/AD) e con il rispetto delle normali procedure di acquisto.

È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

È fatto assoluto divieto di navigare in siti, scaricare, scambiare ed utilizzare materiale pornografico o pedopornografico che possa fare incorrere nei reati di pornografia minorile (art. 600-ter codice penale) e detenzione di materiale pornografico (art. 600-quater codice penale) e così ledere all'immagine di PROVIDENTIA

6.1 Accesso Fortinet Vodafone Rete Unica Diretta (MPLS di VRUD).

Al fine di poter prevenire qualsiasi utilizzo improprio di internet, PROVIDENTIA si è dotata di un sistema di Firewall in Cloud denominato MPLS di VRUD. Tale sistema blocca la navigazione e l'utilizzo dei servizi delle categorie di siti ritenuti non idonei.

Per poter utilizzare internet e i servizi relativi, consentiti dal sistema, è necessario effettuare un accesso, con la propria login di autenticazione, dal un browser ad una qualsiasi pagina internet: il Firewall in Cloud della VRUD effettuerà un redirect verso il pannello di autenticazione.

Utilizzando l'account di dominio LDAP fornito dal *Responsabile Sistema Informatico*, ed effettuando la login (user e password), il dispositivo verrà autorizzato ai servizi internet.

Tale autorizzazione sarà di nuovo necessaria se l'apparato non utilizzerà un servizio internet per almeno 8 ore, quindi di fatto, sarà necessario autenticarsi almeno una volta al giorno.

7. UTILIZZO DI PC PORTATILI

L'utente è responsabile del PC portatile assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai PC portatili si applicano le regole di utilizzo previste per i Pc connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

I PC portatili utilizzati all'esterno (convegni, attività di lavoro fuori sede), in caso di allontanamento, devono essere custoditi in un luogo protetto.

8. USO DELLA POSTA ELETTRONICA

La casella di posta, assegnata dall'Azienda all'utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

È fatto divieto di utilizzare le caselle di posta elettronica aziendale "nome.cognome@lavillaspa.it" per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.

È fatto divieto di utilizzare la posta elettronica aziendale per lo scambio di materiale pornografico o pedopornografico che possa fare incorrere nei reati di pornografia minorile (art. 600-ter codice penale) e detenzione di materiale pornografico (art. 600-quater codice penale) e così ledere all'immagine di PROVIDENTIA

È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per PROVIDENTIA deve essere visionata od autorizzata dal Presidente del CdA/AD, in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.

È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali oppure della posta elettronica certificata (PEC).

È obbligatorio controllare i file attachments di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

È vietato inviare catene telematiche (o di Sant' Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al *Responsabile Sistema Informatico* per poi procedere all'eliminazione degli stessi. Non si devono in alcun caso attivare gli allegati di tali messaggi.

8.1. Disponibilità dei messaggi di posta elettronica.

Il personale di PROVIDENTIA in caso di assenza programmata (ad es. per ferie o attività di lavoro fuori sede), deve adottare le misure organizzative più idonee ad assicurare la corretta gestione dei messaggi necessari al normale svolgimento dell'attività lavorativa ed alla conseguente continuità della stessa.

PROVIDENTIA mette a disposizione di tutti i lavoratori apposite funzionalità di sistema che consentono di impostare un messaggio di risposta automatica (Out of Office Replay). In caso di assenza programmata, l'utente quindi è tenuto ad attivare i messaggi di risposta automatica che comunicano l'assenza dell'utente e devono contenere i riferimenti (sia elettronici che telefonici) di Uffici e/o utenti cui rivolgersi in caso di necessità.

Nel caso, invece, di eventuale assenza improvvisa e/o prolungata (ad es. per malattia) ed il lavoratore non possa attivare la procedura sopra descritta, PROVIDENTIA si riserva la possibilità di attivare analogo accorgimento, avvertendo gli interessati.

Nel caso in cui si preveda la possibilità che, in caso di assenza improvvisa o prolungata, e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica o di altri dati aziendali che siano nella esclusiva disponibilità del dipendente (es. file.PST.), il Responsabile di Area a cui fa capo l'utente, in qualità di fiduciario, può richiedere al Responsabile IT che venga effettuato il reset della password dell'utente stesso. Di tale attività deve essere redatto, a cura del suddetto Responsabile, apposito verbale e deve essere informato l'utente interessato alla prima occasione utile in modo tale da metterlo in condizione di cambiare la password.

L'utente, qualora lo ritenga opportuno, può disporre che il fiduciario sia una persona diversa dal Responsabile di Area/servizio, dandone comunicazione formale all'Ufficio del Responsabile IT, Responsabile in materia di Privacy.

9. ATTIVITÀ DI VERIFICA.

A cura del Responsabile del trattamento dei dati (Presidente CdA) e dell'amministratore del sistema (Responsabile IT) sono periodicamente attivati controlli, anche a campione, al fine di verificare la funzionalità e sicurezza del sistema e garantire l'applicazione del regolamento.

In particolare si rende noto che la società ha attivato sistemi di monitoraggio della navigazione aziendale secondo le previsioni di cui al Provvedimento del Garante Privacy del 1 marzo 2007, effettuando il monitoraggio generalizzato ed anonimo dei log di connessione.

Gli archivi di log risultanti da questo monitoraggio contengono traccia di ogni operazione di collegamento effettuata dall'interno della rete societaria verso Internet.

Eventuali attivazioni di controlli specifici saranno preventivamente comunicate; resta inteso che in caso di anomalie, l'Azienda potrà effettuare verifiche dirette a fini di monitoraggio e controllo delle risorse informatiche, che potranno incidentalmente consentire la conoscibilità dei log di connessione relativi anche ad una sola postazione.

I log di connessione di cui sopra, saranno conservati per 32 gg. decorrenti dalla data di navigazione.

In conformità a quanto previsto dall'atto di nomina dell'Amministratore di Sistema, nei casi in cui si verificano una delle seguenti condizioni:

- prolungata assenza o impedimento dell'incaricato;
- intervento è indispensabile e indifferibile;
- concrete necessità di operatività e di sicurezza del sistema.

L'Amministratore di Sistema può accedere al computer per acquisire i dati necessari al proseguimento dell'attività lavorativa, registrando in apposito verbale le operazioni eseguite.

L'Amministratore di sistema, su propria iniziativa o su richiesta dell'Organismo di Vigilanza, potrà effettuare controlli a campione circa il rispetto di quanto contenuto nel presente regolamento e nel Codice Etico aziendale che ciascun dipendente è tenuto a seguire.

10. CESSAZIONE DEL RAPPORTO DI LAVORO.

In caso di cessazione del rapporto di lavoro, l'utente deve mettere a disposizione di PROVIDENTIA qualsiasi risorsa assegnata, sia le attrezzature informatiche sia le informazioni di interesse aziendale:

- la casella di posta elettronica individuale sarà mantenuta attiva per il tempo strettamente necessario a gestire il passaggio di consegne e concludere eventuali contatti aperti.
- l'utente non può cancellare le informazioni di interesse aziendale presenti sulle postazioni di lavoro e/o sulla rete, senza esplicita autorizzazione del Responsabile di Area/Servizio.
- qualora l'utente abbia inavvertitamente lasciato sulle postazioni di lavoro e/o sulla rete informazioni di interesse non aziendale, le stesse verranno cancellate senza alcuna responsabilità per PROVIDENTIA

11. SANZIONI PER INOSSERVANZA DELLE NORME

Le presenti istruzioni sono impartite ai sensi delle normative vigenti in materia di privacy ed in conformità al Modello di organizzazione, gestione e controllo redatto ai sensi del D.Lgs 231/2001.

L'osservanza delle stesse da parte dell'incaricato può comportare sanzioni anche di natura penale a suo carico ai sensi delle disposizioni di cui alla parte III, cap. I e II del D.lgs n. 196/2003 (artt. da 161 a 172 del

D.lgs. 196/2003) ed ai sensi dell'art. 17 del regolamento di attuazione delle norme in materia di trattamento dei dati personali, emanato con D.R. rep. n. 615 – 2005 del 20/12/2005.

Inoltre si fa presente che l'inosservanza del presente regolamento potrebbe configurare violazione del Codice Etico aziendale e, di conseguenza, essere passibile di sanzioni ai sensi del Codice Sanzionatorio aziendale.

12. AGGIORNAMENTO E REVISIONE

Tutti i dipendenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dalla Direzione (Presidente CdA ed Amministratore Delegato) di concerto con l'Organismo di Vigilanza.

Il presente Regolamento è soggetto a revisione ogni qual volta se ne presenti la necessità. Di ogni revisione successiva sarà data tempestiva comunicazione a tutti i dipendenti.