REGOLAMENTO PER LA PROTEZIONE DEI DATI

Data emissione: 28/11/2018

Versione: 01

INDICE

1 - AMBITO GENERALE 5

1.1 Scopo e campo di applicazione 5

1.2 Destinatari 5

1.3 Autorizzazione all'uso degli strumenti informatici 5

1.4 Finalità nell'utilizzo dei device 6

1.5 Restituzione dei device e dati cartacei 6

2 - MISURE PER L'ACCESSO AI LOCALI 6

2.1 Identificazione delle persone 6

2.2 Custodia delle chiavi fisiche aziendali 6

3 - POSTAZIONE DI LAVORO FISICA E CUSTODIA DI DOCUMENTI CARTACEI 7

4 - GESTIONE DEI DATI E DELLE INFORMAZIONI 7

5 – PASSWORD 7

5.1 Le password 8

5.2 Regole per la corretta gestione delle password 8

5.3 La password nei sistemi 9

5.4 Audit delle password 9

6 - OPERAZIONI A PROTEZIONE DELLA POSTAZIONE DI LAVORO 9

6.1 Login e Logout 9

6.2 Obblighi 9

7 - USO DEL PERSONAL COMPUTER AZIENDALE 10

7.1 Modalità d'uso del computer aziendale 10

7.2 Corretto utilizzo del computer aziendale 10

7.3 Antivirus 10

8 - UTILIZZO DELLE STAMPANTI 11

9 - INTERNET 11

9.1 Internet è uno strumento di lavoro 11

9.2 L'incaricato, nell'utilizzo della rete Internet, deve attenersi alle seguenti regole: 11

9.3 Misure preventive per ridurre navigazioni illecite 12

10 - ACCESSO INTERNET PER TERZI ESTERNI – WIFI GUEST 12

11 - ACCESSO DA REMOTO - VPN ..... Errore. Il segnalibro non è definito.

12 - POSTA ELETTRONICA 12

13 - USO DI ALTRI DEVICE (PERSONAL COMPUTER PORTATILE, TABLET, CELLULARE, SMARTPHONE E DI ALTRI DISPOSITIVI ELETTRONICI) 13

13.1 L'utilizzo del notebook, tablet o smartphone 13

13.2 Utilizzo di supporti di memorizzazione esterne (chiavi usb, hard disk, memory card, dvd, ecc.) 14

13.3 Device personali 14

13.4 Distruzione dei device 14

14 - GESTIONE DI DATI E INFORMAZIONI ATTRAVERSO SISTEMI WEB CLOUD 14

15 - COMUNICAZIONE DI DATI E INFORMAZIONI ATTRAVERSO SOCIAL MEDIA 14

16 - APPLICAZIONE DEL PRESENTE REGOLAMENTO E MONITORAGGIO RETE AZIENDALE 15

16.1 Il controllo 15

16.2 Modalità di verifica 15

16.3 Modalità di conservazione 15

17 - PRESCRIZIONE RESIDUALE 16

18 - PROVVEDIMENTI DISCIPLINARI 16

19 - VALIDITA', AGGIORNAMENTO ED AFFISSIONE 17

19.1 Validità 17

19.2 Aggiornamento 17

19.3 Affissione 17

1 - AMBITO GENERALE

1.1 Scopo e campo di applicazione

Lo scopo del presente regolamento è quello di definire un insieme di norme comportamentali cui tutto il personale (compresi stagisti o tirocinanti), i collaboratori ed eventuali terze parti (di seguito anche "utenti") che operano per Vivai Cooperativi di Padergnone s.c.a. (**da ora "Titolare" o "VICOPAD"**) devono uniformarsi nell'ambito delle attività che implicano:

- l'utilizzo delle strutture informatiche e tecniche che il Titolare, nell'ambito del rapporto instaurato con l'utente e nei termini previsti dal contratto/rapporto di collaborazione, mette a disposizione dello stesso per lo svolgimento della sua attività lavorativa;
- un trattamento di dati ed informazioni personali e aziendali.

Tutto il personale, come sopra identificato, ed ogni consulente esterno che, nell'ambito dell'attività assegnatagli, tratta dati riferiti all'azienda è *Incaricato.*

Le norme di comportamento mirano a far sì che tutti i trattamenti di dati avvengano nel rispetto del Regolamento EU 2016/679, della normativa italiana in materia di dati personali, delle Linee guida del Garante per posta elettronica e internet n. 13/2007 e della normativa giuslavoristica come modificata dal "Jobs Act" del 2015.

1.2 Destinatari

Il presente Regolamento deve essere applicato da tutti gli utenti del Sistema Informatico di VICOPAD, siano essi:

- di dominio:
  - dipendenti/collaboratori
- non di dominio:
  - ospiti esterni che utilizzano internet
  - consulenti informatici per assistenza software
- amministratori (e loro delegati):
  - di dominio (su tutti i pc e tutti i server)
  - di singoli server Linux/Windows
  - del pc (amministratore locale)

1.3 Autorizzazione all'uso degli strumenti informatici

All'inizio del rapporto lavorativo o di consulenza, la cooperativa valuta la presenza dei presupposti per l'autorizzazione all'uso dei vari device aziendali, di Internet e della posta elettronica da parte degli Incaricati per poi, successivamente, valutarne la permanenza.

È fatto esplicito divieto ai soggetti non autorizzati di accedere agli strumenti informatici aziendali.

I casi di esclusione possono riguardare:

A. l'utilizzo del computer o di altri device;
B. l'utilizzo della posta elettronica;
C. l'accesso a Internet.

Le eventuali esclusioni sono strettamente connesse al principio della natura aziendale e lavorativa degli strumenti informatici nonché al principio di necessità di cui al Regolamento Privacy.

Più specificatamente, solo gli Incaricati, per effettivo e concreto bisogno, hanno diritto all'utilizzo degli strumenti e ai relativi accessi.

1.4 Finalità nell'utilizzo dei device

I device assegnati sono uno strumento lavorativo nelle disponibilità dell'Incaricato esclusivamente per un fine di carattere lavorativo. Ciò presuppone che non devono essere utilizzati per finalità private e diverse da quelle aziendali, se non eccezionalmente e nei limiti evidenziati dal presente Regolamento. Qualsiasi eventuale tolleranza da parte di questa cooperativa, apparente o effettiva, non potrà, comunque, legittimare comportamenti contrari alle istruzioni contenute nel presente Regolamento.

È fatta salva in ogni caso la possibilità per la cooperativa di autorizzare l'uso promiscuo di uno o più device.

1.5 Restituzione dei device e dati cartacei

Quando vi è una cessazione del rapporto lavorativo o di consulenza dell'Incaricato con l'organizzazione o del venir meno, ad insindacabile giudizio dell'azienda, della permanenza dei presupposti per l'utilizzo dei device aziendali, gli Incaricati hanno i seguenti obblighi:

1. restituire immediatamente i device in uso;
2. non formattare o alterare o manomettere o distruggere i device e i dati cartacei assegnati o rendere inintelligibili i dati tramite qualsiasi processo.

2 - MISURE PER L'ACCESSO AI LOCALI

2.1 Identificazione delle persone

L'accesso alla sede del Titolare è permesso solo a personale incaricato dalla Direzione in base a precise e motivate esigenze di lavoro.

Le terze parti (fornitori, visitatori, esterni) potranno avere accesso alle aree del Titolare esclusivamente se accompagnate da personale interno.

Il personale interno e le terze parti devono rispettare gli accessi, la fruizione ed il controllo delle aree come definito dalla Direzione.

2.2 Custodia delle chiavi fisiche aziendali

Le chiavi fisiche di accesso alla sede legale sono rilasciate ad alcune figure in base ad esigenze di lavoro, con firma dell'incaricato di ricevuta sull'apposito registro. La gestione di tali chiavi è di responsabilità del dipendente. Tali chiavi devono essere gestite secondo le seguenti indicazioni:

- non devono rimanere incustodite;
- non devono essere cedute a terzi esterni;
- non devono essere duplicate;
- non devono identificare il nome della società;
- il dipendente deve avvisare immediatamente la Direzione in caso di smarrimento o altra anomalia.

3 - POSTAZIONE DI LAVORO FISICA E CUSTODIA DI DOCUMENTI CARTACEI

L'utilizzo della postazione di lavoro e il conseguente accesso ai documenti, atti e archivi è consentito nei limiti della propria funzione e degli incarichi assegnati.

Gli archivi di documenti e atti contenenti dati personali particolari o comunque rischiosi (ad esempio, buste paga, liquidato dei soci) devono essere custoditi in armadi chiusi a chiave.

Sulla propria scrivania non si devono lasciare documenti ed atti riservati e/o contenenti dati particolari senza un proprio controllo all'accesso di terzi, in momenti di pausa, terminata la giornata di lavoro e/o in periodi di assenza.

È necessario rimuovere immediatamente ogni foglio stampato da un'apparecchiatura fax, o acquisito da uno scanner, per evitare che siano prelevati o visionati da soggetti non autorizzati.

Ove possibile, è buona norma eliminare i documenti cartacei contenenti dati e informazioni di natura particolare o riservata attraverso apparecchiature "trita documenti".

4 - GESTIONE DEI DATI E DELLE INFORMAZIONI

Ogni incaricato è responsabile dei dati e delle informazioni personali e aziendali delle quali entra in possesso per lo svolgimento della sua attività lavorativa. Deve quindi trattare i dati e le informazioni adottando ogni idonea misura di sicurezza al fine di tutelarne la riservatezza, la sicurezza ed il corretto utilizzo.

Il trattamento di qualunque dato e informazione personale e aziendale nell'ambito della propria attività lavorativa deve prevedere, da parte del collaboratore incaricato, ogni ragionevole misura per assicurare l'integrità di tali dati. I dati e le informazioni potranno essere comunicati a terze parti esclusivamente nell'ambito della propria funzione e secondo le finalità connesse alla propria attività lavorativa.

È vietata la comunicazione di dati e informazioni a terzi che possano arrecare danno all'immagine, alla reputazione, alla produttività, alla proprietà intellettuale e del know-how ed alla redditività aziendale, che possano violare i vincoli contrattuali e di legge connessi al rapporto di lavoro e che possano ledere i diritti di riservatezza dell'interessato (diritto alla privacy).

È assolutamente vietata la divulgazione a terzi di informazioni sensibili, particolari o riservate o comunque di proprietà del Titolare, senza espressa autorizzazione della Direzione.

In caso di violazione il Titolare si riserva di avviare i relativi provvedimenti disciplinari, nonché le azioni civili e penali consentite.

Gli ospiti vanno fatti attendere in luoghi in cui non sono presenti informazioni riservate o dati personali, premurandosi di abbassare il tono di voce o chiudendo le porte in caso di comunicazioni verbali o telefoniche sensibili.

Qualora si verifichino anomalie, incidenti, furti, perdite accidentali di dati connessi con una ricaduta sul trattamento dei dati personali, al fine di attivare le procedure di comunicazione delle violazioni dei dati (Data Breach) al Garante e agli Interessati, si raccomanda di effettuare immediata segnalazione alla Direzione o al consulente privacy.

5 – PASSWORD

5.1 Le password

Le password rappresentano un metodo di autenticazione assegnato dall'organizzazione per garantire l'accesso protetto ad uno strumento hardware oppure ad un applicativo software.

La prima caratteristica di una password è la segretezza in quanto non deve essere svelata ad altri soggetti. La divulgazione delle proprie password o la trascuratezza nella loro conservazione può essere fonte di gravi danni al proprio lavoro, a quello dei colleghi e dell'azienda nel suo complesso.

È importante ricordare che, nel tempo, anche la password più sicura perde la sua segretezza. Per tal motivo è necessario cambiarle con una certa frequenza.

Altra buona norma è quella di non memorizzare la password su supporti facilmente intercettabili da altre persone. Il miglior luogo in cui conservare una password è la propria memoria.

Qualora il numero di password aziendali da ricordare dovesse diventare eccessivo, si raccomanda l'utilizzo di sistemi di Password Manager, adottati in accordo con l'azienda.

Le password che non vengono utilizzate da parte degli Incaricati per un periodo superiore ai sei mesi verranno disattivate dalla cooperativa.

In qualsiasi momento l'organizzazione si riserva il diritto di revocare all'Incaricato il permesso di accedere ad un sistema hardware o software a cui era precedentemente autorizzato, rimuovendo user id o modificando/cancellando la password ad esso associata.

5.2 Regole per la corretta gestione delle password

L'Incaricato, da parte sua, deve rispettare le seguenti regole per una corretta e sicura gestione delle proprie password:

A. le password sono personali e non vanno mai comunicate ad altri né si deve permettere mai ad altri di utilizzare il proprio account;
B. non autenticarsi al sistema con un account per il cui utilizzo non si è ricevuta una espressa autorizzazione (ad esempio l'account generica di amministratore di sistema);
C. occorre cambiare immediatamente una password nel momento in cui diventa poco "sicura";
D. le password devono essere lunghe almeno 8 caratteri e devono contenere anche lettere maiuscole, caratteri speciali[1] e numeri;
E. le password non devono essere memorizzate su alcun tipo di supporto, quali, ad esempio, post-it (sul monitor o sotto la tastiera) o agende (cartacee, posta elettronica, telefono cellulare);
F. le password devono essere sostituite almeno ogni sei mesi, a prescindere dall'esistenza di un sistema automatico di richiesta di aggiornamento password;
G. le password devono essere digitate in assenza di altri soggetti, i quali potrebbero vedere la tastiera, anche se collaboratori o dipendenti dell'cooperativa.
H. non utilizzare come propria password: nome, cognome e loro parti; lo username assegnato; un indirizzo di posta elettronica (e-mail); parole comuni o frasi di senso compiuto (in qualsiasi lingua), come si possono trovare su un dizionario o sul web; date, mesi dell'anno e giorni della settimana, anche in lingua straniera; parole banali e/o di facile intuizione; ripetizioni di sequenze di caratteri (es. abcabcabc).

[1] Per caratteri speciali si intendono, per esempio, i seguenti: { } [ ] , . < > ; : ! " £ $ % & / ( ) = ? ^ \ | ' * - + _.

Si ricorda che, in alcuni casi, sono implementati meccanismi che consentono all'Incaricato fino ad un numero limitato di tentativi errati di inserimento della password oltre ai quali il tentativo di accesso viene considerato un attacco al sistema e l'account viene bloccato per alcuni minuti. In caso di necessità contattare il Titolare.

5.3 La password nei sistemi

Ogni Incaricato può modificare la propria password di accesso a qualsiasi sistema della cooperativa in modo autonomo, qualora il sistema in questione metta a disposizione degli Utenti una funzionalità di questo tipo (change password), oppure facendone richiesta al Titolare. In generale, la password può essere sostituita dalla cooperativa, anche qualora l'Utente l'abbia dimenticata.

5.4 Audit delle password

Nell'ambito delle attività riguardanti la tutela della sicurezza della infrastruttura tecnologica, la cooperativa potrebbe effettuare analisi periodiche sulle password degli Incaricati al fine di verificarne la solidità, le policy di gestione e la durata, informandone preventivamente gli Incaricati stessi.

Nel caso in cui l'audit abbia, tra gli esiti possibili, la decodifica della password, questa viene bloccata e all'Incaricato richiesto di cambiarla.

6 - OPERAZIONI A PROTEZIONE DELLA POSTAZIONE DI LAVORO

6.1 Login e Logout

Il "login" è l'operazione con la quale l'Incaricato si connette al sistema informativo aziendale o ad una parte di esso, dichiarando il proprio Username e Password (ossia l'Account), aprendo una sessione di lavoro. In molti casi è necessario effettuare più login, tanti quanti sono gli ambienti di lavoro (ad es. applicativi web, Intranet), ognuno dei quali richiede un username e una password.

In questi casi, sebbene sia preferibile che ogni utente abbia un suo specifico user name e password, la cooperativa potrà assegnare un univoco user name e password per gruppi di Incaricati per l’accesso alla macchina fisica, mentre rimarranno generalmente separati ed univoci per l’accesso agli applicativi che contengono dati.

Il "logout" è l'operazione con cui viene chiusa la sessione di lavoro. Al termine della giornata lavorativa, tutte le applicazioni devono essere chiuse secondo le regole previste dall'applicazione stessa in quanto la non corretta chiusura può provocare una perdita di dati o l'accesso agli stessi da parte di persone non autorizzate.

Il "blocco del computer" è l'operazione con cui viene impedito l'accesso alla sessione di lavoro (tastiera e schermo disattivati) senza chiuderla.

6.2 Obblighi

L'utilizzo dei dispositivi fisici e la gestione dei dati ivi contenuti devono svolgersi nel rispetto della sicurezza e dell'integrità del patrimonio dati aziendale.

L’incaricato deve quindi eseguire le operazioni seguenti:

a) se si allontana dalla propria postazione dovrà mettere in protezione il suo device per evitare che persone non autorizzate abbiano accesso ai dati protetti (attivazione, anche automatica, dello screen saver con password);
b) chiudere la sessione (Logout) a fine giornata;

c) spegnere il PC dopo il Logout;
d) controllare che non vi siano persone non autorizzate alle sue spalle che possano prendere visione delle schermate del suo device.

7 - USO DEL PERSONAL COMPUTER AZIENDALE

7.1 Modalità d'uso del computer aziendale

Il sistema informativo aziendale è costituito da un computer utilizzato come FileServer e altri computer client connessi ad una rete locale (LAN), che utilizzano diversi sistemi operativi e applicativi.

I file creati, elaborati o modificati sul computer assegnato devono essere sempre salvati sul server o file system centralizzato, ove disponibile, poiché la Cooperativa non effettua il backup dei dati memorizzati in locale.

Tutti gli incaricati, quindi, non devono salvare i documenti importanti solamente sul proprio PC, ma sulle cartelle di rete oggetto di back up.

7.2 Corretto utilizzo del computer aziendale

Il computer consegnato all'incaricato è uno strumento di lavoro e contiene tutti i software necessari a svolgere le attività affidate. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, rallentamenti del sistema, costi di manutenzione e, soprattutto, minacce alla sicurezza.

Non è quindi consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal Titolare. Di conseguenza non è consentito all'incaricato installare autonomamente alcun programma informatico senza la previa autorizzazione della Direzione o dell'Amministratore di Sistema. 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 (*Decreto Legislativo 518/92 sulla Tutela giuridica del software e Legge 248/2000 Nuove norme di tutela del diritto d'autore*). È inoltre vietato immettere sulla rete e server aziendali software dannosi per i sistemi o comunque non autorizzati.

Non è poi consentito all'incaricato modificare le caratteristiche impostate sul proprio PC o Notebook, né procedere ad installare software, dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, etc.) senza autorizzazione.

Per quanto attiene più specificatamente al trattamento dei dati, all'incaricato, infine, è vietato:

a) accedere ai dati sulla rete aziendale per i quali non si è stati espressamente autorizzati;
b) eseguire qualsiasi azione di monitoraggio della rete al fine di intercettare dati che non sono destinati alla propria postazione;
c) eludere il processo di autenticazione o di sicurezza previsto per ogni postazione, rete o account;
d) caricare sul disco fisso del computer o nel server alcun documento, gioco, file musicale o audiovisivo o immagine diversi da quelli necessari allo svolgimento delle mansioni affidate;
e) accedere, rivelare o utilizzare informazioni non autorizzate o comunque non necessarie per le mansioni svolte;
f) usare il pc aziendale per procurarsi o trasmettere materiale che è in violazione alle leggi vigenti.

7.3 Antivirus

I virus possono essere trasmessi tramite scambio di file via Internet, via mail, scambio di supporti removibili, file sharing, chat, etc.

La gestione (installazione, aggiornamento, etc.) del software antivirus è di competenza di chi il Titolare ha incaricato in tal senso. Tuttavia, è necessario che ogni incaricato presti attenzione ad eventuali anomalie e/o avvisi dal sistema antivirus ed eviti di disabilitare, per qualsiasi motivo, il sistema antivirus. L'incaricato, inoltre, deve comunicare ogni anomalia o malfunzionamento del sistema antivirus e la presenza di virus o file sospetti.

Infine, è vietato aprire allegati di mail provenienti da mittenti sconosciuti o di dubbia provenienza o allegati di mail di persone conosciute ma con testi sospetti, incongrui o in qualche modo strani.

8 - UTILIZZO DELLE STAMPANTI

È vietato l'utilizzo per fini personali dei sistemi multifunzione (sistemi di stampa, copia ed invio fax) e dei sistemi fax aziendali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte della Direzione.

Si raccomanda di non lasciare documenti contenenti dati personali incustoditi presso i suddetti dispositivi.

9 - INTERNET

9.1 Internet è uno strumento di lavoro

L'accesso ad Internet (*tramite PC, tablet o smartphone aziendali*) è fornito allo scopo di consentire l'accesso alle informazioni necessarie all'attività lavorativa. Essendo uno strumento di lavoro, gli utenti cui si attribuisce l'accesso sono responsabili del suo corretto utilizzo.

L'utilizzo per scopi personali è tollerato in via eccezionale e con gli accorgimenti di cui al presente documento. In particolare, si vieta l'utilizzo dei social network, se non espressamente autorizzati.

Si informa che il numero, la durata ed il contenuto degli accessi ad Internet possono essere costantemente registrati. La consultazione di tali registrazioni può avvenire solo in forma anonima e aggregata salvo i casi previsti dalla legge. Per prevenire eventuali abusi nell'uso di Internet, il sistema è provvisto di filtri d'accesso.

9.2 L'incaricato, nell'utilizzo della rete Internet, deve attenersi alle seguenti regole:

- è tassativamente vietato scaricare materiale e programmi in violazione della legislazione sui diritti di autore, che siano essi appartenenti a persone o aziende, coperti da *copyright*, brevetto o proprietà intellettuale, ivi compresa l'installazione o la distribuzione di software che non sia specificatamente licenziato per essere utilizzato all'interno dell'azienda;
- è tassativamente vietato navigare siti e scaricare materiale vietato o aventi contenuti illegali;
- è vietato effettuare copia non autorizzata di materiale coperto da copyright compreso, ma non limitato a, digitalizzazione e distribuzione di foto da riviste, libri o altre fonti, musica o materiale video;
- è vietata la condivisione di file in modalità peer-to-peer;

- è vietato scaricare programmi, anche se privi di licenza o in prova (*freeware e shareware*), se non in caso di espressa autorizzazione dell'Amministratore di sistema. Eseguire il download di file da Internet è infatti un'operazione pericolosa in quanto può essere il veicolo per l'introduzione di *virus e malware*;
- è vietato utilizzare l'infrastruttura tecnologica aziendale per procurarsi e diffondere materiale in violazione delle normative vigenti;
- è vietato eseguire qualsiasi forma di monitoraggio della rete che permetta di catturare dati non espressamente inviati *all'host* dell'utente (*sniffing*);
- è vietato aggirare le procedure di autenticazione o la sicurezza di qualunque *host*, rete, *account*;
- è vietato l'utilizzo in rete di PC fissi, portatili, tablet e smartphones personali, salvo espressa autorizzazione da parte della Direzione.

9.3 Misure preventive per ridurre navigazioni illecite

L'organizzazione potrà adottare idonee misure tecniche preventive volte a ridurre navigazioni a siti non correlati all'attività lavorativa attraverso filtri e black list.

10 - ACCESSO INTERNET PER TERZI ESTERNI – WIFI GUEST

È previsto un sistema per consentire l'accesso ad Internet a terzi esterni. L'accesso alla rete (*tramite PC, tablet o smartphone*) è fornito allo scopo di consentire la navigazione a clienti, fornitori, terzi esterni e non a utenti interni. Gli utenti cui si attribuisce l'accesso tramite password sono responsabili del suo corretto utilizzo. Si informa che il numero, la durata ed il contenuto degli accessi ad Internet sono costantemente registrati.

12 - POSTA ELETTRONICA

L'assegnazione di una casella e-mail (personale o di gruppo) è finalizzata all'utilizzo della stessa esclusivamente per finalità legate alle attività lavorative. Gli utenti della posta elettronica sono responsabili del corretto utilizzo della stessa e devono mantenere un corretto comportamento nell'utilizzo dello strumento di posta elettronica, sia nei messaggi inviati internamente che esternamente.

In particolare, devono essere seguite le seguenti disposizioni:

- i messaggi di posta diretti a destinatari esterni dell'organizzazione, devono contenere il seguente disclaimer

  "Questo messaggio (e-mail e tutti gli allegati) è confidenziale e si intende inviato esclusivamente ai destinatari. Eventuali trattamenti relativi ai dati personali contenuti verranno compiuti nel rispetto del GDPR 2016/679. La diffusione, la distribuzione e/o la copiatura del documento trasmesso da parte di qualsiasi soggetto diverso dal destinatario è proibita ai sensi dell'art. 616 c.p.. Se avete ricevuto questa e-mail per errore, siete pregati di eliminarla in ogni sua parte e di avvisare possibilmente il mittente."

- la casella di posta elettronica aziendale (personale o di gruppo) non deve essere utilizzata per l'invio o la ricezione di messaggi personali al di fuori dalle finalità lavorative o per la partecipazione a dibattiti, forum o mailing-list, salvo diversa ed esplicita autorizzazione della Direzione;
- non inviare né conservare messaggi di posta elettronica e/o allegati dal contenuto offensivo, molesto, volgare, blasfemo, xenofobo, razziale, pornografico o comunque inappropriato o illegale;

- deve essere prestata la massima attenzione nell'inoltro di mail riportanti contenuti e indirizzi e-mail di precedenti comunicazioni;
- in caso di assenza prolungata (ferie, malattia, aspettativa, lunga attività fuori sede) l'utente deve prevedere delle opportune procedure, in collaborazione con la Dirigenza o l'Amministrazione, in grado di garantire la continuità delle attività. In generale, sarebbe buona norma attivare il servizio di risposta automatica (Auto-reply). In alternativa ed in tutti i casi in cui sia necessario un presidio della casella di e-mail per ragioni di operatività aziendale, l'Incaricato deve nominare "vice" un collega fiduciario che in caso di assenza inoltri i file necessari a chi ne abbia urgenza. Qualora l'Incaricato non abbia provveduto ad individuare un collega fiduciario o questi sia assente o irreperibile, l'organizzazione, mediante personale appositamente incaricato, potrà verificare il contenuto dei messaggi di posta elettronica dell'incaricato, informandone l'incaricato stesso.

Si avvisano gli utenti che:

- tutta la posta elettronica in entrata è controllata da un software antispam. È comunque possibile che alcune mail di spam superino i filtri impostati sul sistema centrale: quindi è necessario prestare la massima attenzione a e-mail sospette, avvisando la direzione in caso di dubbi sulla provenienza/contenuto delle stesse;
- tutti i messaggi ricevuti, spediti o salvati, potranno essere letti della Direzione esclusivamente nei seguenti casi:
    a. in caso di improvvisa assenza dell'utente al fine di garantire una regolare continuità dell'attività lavorativa;
    b. per motivi di sicurezza informatica.

In questi casi sarà data informazione all'utente dell'accesso eseguito.

13 - USO DI ALTRI DEVICE (PERSONAL COMPUTER PORTATILE, TABLET, CELLULARE, SMARTPHONE E DI ALTRI DISPOSITIVI ELETTRONICI)

13.1 L'utilizzo del notebook, tablet o smartphone

L'organizzazione può concedere in uso il computer portatile, il tablet e il cellulare (di seguito generalizzati in "device mobile") agli Incaricati che necessitano di disporre di archivi elettronici, supporti di automazione e/o di connessione alla rete dell'organizzazione durante gli spostamenti. L'Incaricato è responsabile dei device mobili assegnatigli dall'organizzazione, ha il compito di custodirli con diligenza e, di norma, non deve esserne consentito l'utilizzo da parte di terzi.

Ai device mobili si applicano le regole di utilizzo previste per i computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna. In particolare, i file creati o modificati sui device mobili devono essere trasferiti sulle memorie di massa aziendali al primo rientro in ufficio e cancellati in modo definitivo dai device mobili (Wiping).

Sui device mobili è vietato installare applicazioni (anche gratuite) se non espressamente autorizzate dall'azienda. I device mobili utilizzati all'esterno (convegni, visite, ecc…), in caso di allontanamento, devono essere custoditi in un luogo protetto.

In caso di perdita o furto deve seguire la denuncia alle autorità competenti e avvisare immediatamente l'azienda che provvederà – se del caso – ad occuparsi delle procedure connesse alla privacy. Anche di giorno, durante l'orario di lavoro, l'Incaricato non deve lasciare incustoditi i device mobili.

L'Incaricato, inoltre, non deve lasciare i device mobili incustoditi in ambienti pubblici (in vista dentro l'auto, in una stanza d'albergo, nell'atrio dell'albergo o nelle sale d'attesa delle stazioni ferroviarie e aeroportuali).

I device mobili che permettono l'attivazione di una procedura di protezione (PIN o gesture) devono sempre essere abilitabili solo con tale procedura di protezione. Se disponibile, è raccomandata la cifratura del device.

13.2 Utilizzo di supporti di memorizzazione esterne (chiavi usb, hard disk, memory card, dvd, ecc.)

Al termine dell'utilizzo dei supporti di memorizzazione contenenti dati (chiavette USB, Hard Disk interni ed esterni), questi devono essere cancellati, per eliminare ogni informazione contenuta prima di autorizzarne qualunque tipo di nuovo utilizzo.

13.3 Device personali

Ai dipendenti non è permesso svolgere la loro attività su PC fissi, portatili, device di proprietà personale (Bring Your Own Device - BYOD) ad eccezione dell'utilizzo della posta elettronica aziendale, quando espressamente autorizzati dall'azienda. In questo caso è necessario che il device abbia password di sicurezza stringenti e l'eventuale furto o smarrimento deve essere immediatamente segnalato anche all'azienda per eventuali provvedimenti di sicurezza.

Al collaboratore è vietato l'utilizzo di memorie esterne personali (quali chiavi USB, memory card, cd-rom, DVD, macchine fotografiche, videocamere, tablet, …).

I consulenti e collaboratori esterni possono utilizzare i propri device personali per memorizzare dati dell'azienda solo se espressamente autorizzati dall'azienda stesso e assumendone formalmente e personalmente l'intera responsabilità del trattamento.

13.4 Distruzione dei device

Ogni device ed ogni memoria esterna affidati agli Incaricati, (computer, notebook, tablet, smartphone, memory card, chiavi usb, hard disk, dvd, cd-rom, ecc.), al termine del loro utilizzo dovranno essere restituiti alla cooperativa che provvederà a ricondizionarli o eventualmente a distruggerli seguendo le norme di legge in vigore al momento.

In particolare, la cooperativa provvederà a cancellare o a rendere inintelligibili i dati negli stessi memorizzati.

14 - GESTIONE DI DATI E INFORMAZIONI ATTRAVERSO SISTEMI WEB CLOUD

È vietato il salvataggio di dati e informazioni di carattere aziendale in sistemi *cloud* (per esempio *Dropbox, Google+, iCloud, Evernote, etc.*) non autorizzati dalla Direzione e dall'Amministratore di sistema.

15 - COMUNICAZIONE DI DATI E INFORMAZIONI ATTRAVERSO SOCIAL MEDIA

È assolutamente vietato pubblicare in internet attraverso Social media personali, forum, chat, blog, siti internet, dati ed informazioni riguardanti la cooperativa e relativo al personale dipendente (informazioni, documenti, appunti, commenti personali o di terzi, foto, video, audio, etc.) non autorizzati dalla Direzione aziendale.

È invece autorizzata la divulgazione di informazioni già rese pubbliche dall'azienda.

16 - APPLICAZIONE DEL PRESENTE REGOLAMENTO E MONITORAGGIO RETE AZIENDALE

16.1 Il controllo

L'azienda, in qualità di Titolare degli strumenti informatici, dei dati ivi contenuti e/o trattati, si riserva la facoltà di effettuare i controlli che ritiene opportuni per le seguenti finalità:

a. tutelare la sicurezza e preservare l'integrità degli strumenti informatici e dei dati;
b. evitare la commissione di illeciti o per esigenze di carattere difensivo anche preventivo.
c. verificare la funzionalità del sistema e degli strumenti informatici e mantenerne la funzionalità.

Le attività di controllo potranno avvenire anche con audit e vulnerability assesment del sistema informatico. Per tali controlli l'organizzazione si riserva di avvalersi di soggetti esterni.

Si precisa, in ogni caso, che l'organizzazione non adotta "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori" (ex art. 4, primo comma, l. n. 300/1970), tra cui sono certamente comprese le strumentazioni hardware e software mirate al controllo dell'utente.

16.2 Modalità di verifica

Periodicamente e in presenza di anomalie (intervento antivirus, segnalazione di rallentamenti del computer, utilizzo aziendalmente eccessivo dell'accesso Internet, dimensione elevata della casella di posta elettronica o dello spazio disco utilizzato, etc.), l'amministratore di sistema effettuerà verifiche di funzionalità approfondite che potranno determinare segnalazione ed avvisi generalizzati diretti ai dipendenti della funzione in cui è stata rilevata l'anomalia stessa e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie.

In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

16.3 Modalità di conservazione

I sistemi software sono stati programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

Un eventuale prolungamento dei tempi di conservazione viene valutato come eccezionale e deve aver luogo solo in relazione:

a. ad esigenze tecniche o di sicurezza del tutto particolari;
b. all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
c. all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

In questi casi, il trattamento dei dati personali è limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

17 - PRESCRIZIONE RESIDUALE

L'utente è tenuto a custodire con cura gli strumenti affidatigli, segnalando tempestivamente alla direzione eventuali anomalie, guasti o smarrimenti.

Per dubbi ed incertezze, in merito a come debba avvenire il trattamento dei dati e delle informazioni personali e aziendali, nonché sulle modalità di utilizzo degli strumenti di trattamento, è possibile chiedere alla Direzione o all'Amministratore di sistema o al consulente privacy per ricevere le opportune istruzioni.

18 - PROVVEDIMENTI DISCIPLINARI

Le infrazioni disciplinari alle norme del presente Regolamento Interno potranno essere punite, a seconda della gravità delle mancanze, in conformità alle disposizioni di legge e/o del Contratto Collettivo Nazionale del Lavoro applicato, tra cui:

a. il biasimo inflitto verbalmente;
b. lettera di richiamo inflitto per iscritto;
c. multa;
d. la sospensione dalla retribuzione e dal servizio;
e. il licenziamento disciplinare e con le altre conseguenze di ragioni e di legge.

Per i dirigenti valgono le vigenti norme di legge e/o di contrattazione collettiva, fermo restando che, per le violazioni di maggior gravità l'azienda potrà procedere al licenziamento del dirigente autore dell'infrazione.

19 - VALIDITA’, AGGIORNAMENTO ED AFFISSIONE

19.1 Validità

Il presente Regolamento ha validità a partire dal 28/11/2018.

19.2 Aggiornamento

Il presente Regolamento **sarà oggetto di aggiornamento ogni volta che se ne ravvisi la necessità**, **in caso di variazioni tecniche dei sistemi dell’organizzazione o in caso di mutazioni legislative**.

Ogni variazione del presente Regolamento sarà comunicata agli Incaricati.

19.3 Affissione

Il presente Regolamento costituisce parte integrante del regolamento disciplinare aziendale – cui dovrà essere allegato - e verrà affisso nella bacheca aziendale ed eventualmente pubblicato sulla intranet aziendale ai sensi dell’art. 7 della legge 300/70 e del CCNL.