25 maggio 2018

LICEO "ARIOSTO – SPALLANZANI"

PROCEDURA OPERATIVA

AMBITO GENERALE
GESTIONE DELLE PASSWORD
GESTIONE OPERAZIONI A PROTEZIONE DELLA POSTAZIONE DI LAVORO
GESTIONE USO DEL PERSONAL COMPUTER DELL'ENTE
GESTIONE INTERNET
GESTIONE POSTA ELETTRONICA
GESTIONE SISTEMI IN CLOUD
GESTIONE DATI CARTACEI
CONSEGNA DEVICE PER INTERRUZIONE DEL RAPPORTO DI LAVORO
PROVVEDIMENTI DISCIPLINARI
VALIDITÀ, AGGIORNAMENTO ED AFFISSIONE
MODULO – DATA BREACH

Via Aristotele, 109 – 42122 Reggio Emilia (RE)
Tel. 0522-087829
www.01privacy.it – info@01privacy.it
P.IVA 02786920351

AMBITO GENERALE

Premessa

L’ambito lavorativo porta la nostra organizzazione a gestire una serie di “**informazioni**”, proprie e di terzi, per poter erogare i servizi che le vengono contrattualmente richiesti.
Tali informazioni possono essere considerate, ai sensi del Regolamento Europeo UE 2016/679 “**dati personali**” quando sono riferite a persone fisiche e, per la loro gestione (Trattamento), sia cartacea che digitale, è necessario che l’ente adotti una serie di misure minime ed idonee previste dalle norme.
Altre informazioni, pur non essendo “dati personali” ai sensi di legge, sono in tutto e per tutto “**informazioni riservate**”, ovvero informazioni tecniche, commerciali, contrattuali, di business o di altro genere per le quali l’organizzazione è chiamata a garantire la riservatezza, o per NDA, o per una più ampia tutela del patrimonio aziendale.
Ai fini di questo disciplinare si specifica, pertanto, che con il termine “**dati**” deve intendersi l’insieme più ampio di informazioni di cui un dipendente o un collaboratore può venire a conoscenza e di cui deve garantire la riservatezza e la segretezza e non solo i “dati personali” intesi a norma di legge.
Inoltre, nell’ambito della sua attività, l’ente tratta “**dati cartacei**” ovvero informazioni su supporto cartaceo e “**dati digitali**” ovvero informazioni che vengono memorizzate o semplicemente transitano attraverso apparecchiature digitali.
In linea generale, ogni dato, nell’accezione più ampia sopra descritta, di cui l’incaricato viene a conoscenza, nell’ambito della propria attività lavorativa, è da considerarsi riservato e non deve essere comunicato o diffuso a nessuno (anche una volta interrotto il rapporto lavorativo con l’organizzazione stessa o qualora parte delle informazioni siano di pubblico dominio) salvo specifica autorizzazione esplicita dell’ente.
Anche tra colleghi, oppure tra dipendenti e collaboratori esterni, è necessario adottare la più ampia riservatezza nella comunicazione dei dati conosciuti, limitandosi solo a quei casi che si rendono necessari per espletare al meglio l’attività lavorativa richiesta.
La progressiva diffusione delle nuove tecnologie informatiche ed in particolare l’accesso alla rete internet dal computer aziendale espone l’ente a possibili rischi di un coinvolgimento di rilevanza sia civile, sia penale, sia amministrativa, creando problemi alla sicurezza e all’immagine dell’organizzazione stessa.
Premesso che i comportamenti che normalmente si adottano nell’ambito di un rapporto di lavoro, tra i quali rientrano l’utilizzo delle risorse informatiche e telematiche, devono sempre ispirarsi al principio di diligenza e correttezza, l’ente ha adottato il presente Disciplinare Interno diretto ad evitare che condotte inconsapevoli possano innescare problemi o minacce alla sicurezza dei dati o delle attrezzature aziendali.
Il presente Disciplinare Interno si applica agli **autorizzati** che si trovino ad operare con dati dell’ente.
Una gestione dei dati cartacei, un uso dei COMPUTER e di altri dispositivi elettronici (di seguito DEVICE) nonché dei servizi di internet e della posta elettronica difforme dalle regole contenute nel presente Disciplinare potrebbe esporre l’organizzazione ad aumentare la minaccia di accessi non autorizzati ai dati e/o al sistema informatico aziendale, furti o divulgazioni di informazioni riservate nonché furti o danneggiamenti del sistema informatico e/o malfunzionamenti in generale dell’intero sistema informatico.
Le informazioni contenute nel presente Disciplinare vengono rilasciate anche ai sensi dell’art. 13 del Regolamento Europeo UE 2016/679 e costituiscono, quindi, parte integrante dell’informativa rilasciata.

GESTIONE DELLE PASSWORD

1. Premessa

Le password possono essere 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**, cioè il fatto che non venga svelata ad altri soggetti. La divulgazione delle proprie password o la trascuratezza nella loro conservazione possono causare gravi danni al proprio lavoro, a quello dei colleghi e dell'ente nel suo complesso.
Nel tempo anche la password più sicura perde la sua segretezza. Per questo motivo è buona norma cambiarle con una certa frequenza.
Per una gestione ottimale dei sistemi informatici l'ente potrebbe implementare alcuni meccanismi che permettano di aiutare e supportare gli Incaricati in una corretta gestione delle password, in particolare, per quanto riguarda le password di accesso al Dominio (ove previsto), si potrebbe prevedere un sistema automatico di richiesta di aggiornamento delle stesse impostato dall’ente secondo il livello di sicurezza richiesto dall’ente stesso e, comunque, in linea con quanto richiesto dalla normativa privacy.
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.
Le password che non vengono utilizzate da parte degli incaricati per un periodo superiore ai sei mesi dovrebbero essere disattivate dall’ente.
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.

2. Regole per la corretta gestione delle password

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

1. Le password sono assolutamente personali e non vanno mai comunicate ad altri;
2. Occorre cambiare immediatamente una password non appena si abbia alcun dubbio che sia diventata poco "sicura";
3. Le password devono essere lunghe almeno 8 caratteri e devono contenere anche lettere maiuscole, caratteri speciali [1]e numeri;
4. 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);
5. Le password devono essere sostituite almeno nei tempi indicati dalla normativa, a prescindere dall'esistenza di un sistema automatico di richiesta di aggiornamento password.
6. Evitare di digitare la propria password in presenza di altri soggetti che possano vedere la tastiera, anche se collaboratori o dipendenti dell’ente.

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

Si può valutare di implementare 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.

3. Divieto di uso

Al fine di una corretta gestione delle password, è bene evitare, come propria password:

1. Nome, cognome e loro parti;
2. Lo username assegnato;
3. Un indirizzo di posta elettronica (e-mail);
4. Parole comuni (in Inglese e in Italiano);
5. Date, mesi dell'anno e giorni della settimana, anche in lingua straniera;
6. Parole banali e/o di facile intuizione, ad es. pippo, security e palindromi (simmetria: radar);
7. Ripetizioni di sequenze di caratteri (es. abcabcabc);
8. Una password già impiegata in precedenza.

3.1 Alcuni esempi di password non ammesse

La password ideale deve essere complessa, senza alcun riferimento, ma facile da ricordare.
Una possibile tecnica è usare sequenze di caratteri prive di senso evidente, ma con singoli caratteri che formano una frase facile da memorizzare (es.: "NIMzz5DICmm!", Nel Mezzo Del Cammin, più il carattere 5 e il punto esclamativo).
Decifrare una parola come questa può richiedere giorni, una come "*radar*" meno di dieci secondi.

Alcuni esempi di password assolutamente da evitare:

1. Se Username = "mariorossi", password = "mario", o ancora peggio, password = "mariorossi";
2. Il nome della moglie/marito, fidanzato/a, figli, ecc. anche a rovescio;
3. La propria data di nascita, quella del coniuge, ecc.;
4. Targa della propria auto;
5. Numero di telefono proprio, del coniuge, ecc.;
6. Parole comuni tipo "Kilimangiaro", “Password”, “Qwerty”, “12345678” (troppo facili);
7. Qualsiasi parola del vocabolario (di qualsiasi lingua diffusa, come inglese, italiano, ecc.).

4. La password nei sistemi

Ogni Incaricato può variare la propria password di accesso a qualsiasi sistema aziendale 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.
La password può essere sostituita dal Titolare, anche qualora l'Utente l'abbia dimenticata.

5. Audit delle password

Nell'ambito delle attività riguardanti la tutela della sicurezza della infrastruttura tecnologica, l'ente 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.

GESTIONE OPERAZIONI A PROTEZIONE DELLA POSTAZIONE DI LAVORO

1. Premessa

In questa sezione vengono trattate le operazioni a carico dell’Incaricato e il quadro di riferimento generale per l'esecuzione di operazioni a protezione della propria postazione di lavoro, nel rispetto della sicurezza e dell'integrità del patrimonio aziendale.

2. 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 username e password, l’Ente potrà assegnare un univoco username e password per gruppi di incaricati per l’accesso alla macchina fisica, mentre rimarranno 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.
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.

3. 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:

1. Se si allontana dalla propria postazione dovrà mettere in protezione il suo device affinché persone non autorizzate non abbiano accesso ai dati protetti.
2. Bloccare il suo device prima delle pause e, in generale, ogni qualvolta abbia bisogno di allontanarsi dalla propria postazione;
3. Chiudere la sessione (Logout) a fine giornata;
4. Spegnere il PC dopo il Logout;
5. Controllare sempre che non vi siano persone non autorizzate alle sue spalle che possano prendere visione delle schermate del suo device.

GESTIONE USO DEL PERSONAL COMPUTER DELL’ENTE

1. Modalità d’uso del COMPUTER aziendale

I *files* creati, elaborati o modificati sul computer assegnato devono essere poi sempre salvati a fine giornata sul sistema di repository documentale centralizzato (se presente).

2. Corretto utilizzo del COMPUTER aziendale

Il computer consegnato agli autorizzati 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.
L’accesso all’elaboratore è protetto da password che deve essere custodita dall’autorizzato con la massima diligenza e non divulgata.
Il computer che viene consegnato contiene tutti i software necessari a svolgere le attività affidate dall’organizzazione.
Per necessità aziendali, gli amministratori di sistema utilizzando la propria login con privilegi di amministratore e la password dell’amministratore, potranno accedere, con le regole indicate nel presente documento, sia alla memoria di massa locali di rete (repository e backup) che ai server aziendali nonché, previa comunicazione al dipendente, accedere al computer, anche in remoto.

In particolare l’autorizzato deve adottare le seguenti misure:

1. Utilizzare solo ed esclusivamente le aree di memoria della rete dell’ente ed ivi creare e registrare file e software o archivi dati, senza pertanto creare altri *files* fuori dalle unità di rete;
2. Spegnere il computer, o curarsi di effettuare il *Logout*, ogni sera prima di lasciare gli uffici o in caso di assenze prolungate, poiché 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;
3. Mantenere sul computer esclusivamente i dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori), disposti dall’organizzazione;
4. Non dare accesso al proprio computer ad altri utenti, a meno che siano incaricati con cui condividono l’utilizzo dello stesso Pc o a meno di necessità stringenti e sotto il proprio costante controllo.

3. Divieti Espressi sull’utilizzo del COMPUTER

All’autorizzato è vietato:

1. La gestione, la memorizzazione (anche temporanea) o il trattamento di file, documenti e/o informazioni personali dell’autorizzato o comunque non afferenti alle attività lavorative nella rete, nel disco fisso o in altre memorie di massa aziendali e negli strumenti informatici aziendali in genere.
2. Modificare le configurazioni già impostate sul personal computer.
3. Utilizzare programmi e/o sistemi di criptazione senza la preventiva autorizzazione scritta dell’ente.
4. Installare alcun software di cui l’ente non possieda la licenza, né installare alcuna versione diversa, anche più recente, rispetto alle applicazioni o al sistema operativo presenti sul personal computer consegnato, senza l’espressa autorizzazione dell’organizzazione. Né è, peraltro, consentito fare copia del software installato al fine di farne un uso personale.
5. 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.
6. Aggiungere o collegare dispositivi hardware (ad esempio hard disk, driver ecc.) o periferiche (telecamere, macchine fotografiche, smartphone, chiavi USB ecc.) diversi da quelli consegnati, senza l’autorizzazione espressa dell’organizzazione.
7. Creare o diffondere, intenzionalmente o per negligenza, programmi idonei a danneggiare il sistema informatico dell’organizzazione, quali per esempio virus, trojan horses ecc.

8. Accedere, rivelare o utilizzare informazioni non autorizzate o comunque non necessarie per le mansioni svolte.
9. Effettuare in proprio attività manutentive.
10. Permettere attività manutentive da parte dei soggetti non espressamente autorizzati dell’organizzazione.

4. Antivirus

I virus possono essere trasmessi tramite scambio di file via internet, via mail, scambio di supporti removibili, filesharing, chat, via mail …
L'ente impone su tutte le postazioni di lavoro l'utilizzo di un sistema antivirus correttamente installato, attivato continuamente e aggiornato automaticamente con frequenza almeno quotidiana.
L’autorizzato, da parte sua, deve impegnarsi a controllare il corretto funzionamento e aggiornamento del sistema antivirus installato sul proprio computer, e, in particolare, deve rispettare le regole seguenti:

1. Comunicare all’ente ogni anomalia o malfunzionamento del sistema antivirus;
2. Comunicare all’ente eventuali segnalazioni di presenza di virus o file sospetti.

Inoltre, all’incaricato:

1. È vietato accedere alla rete aziendale senza servizio antivirus attivo e aggiornato sulla propria postazione;
2. È vietato ostacolare l'azione dell'antivirus aziendale;
3. È vietato disattivare l’antivirus senza l’autorizzazione espressa dell’ente anche e soprattutto nel caso sia richiesto per l’installazione di software sul computer;
4. È vietato aprire allegati di mail provenienti da mittenti sconosciuti o di dubbia provenienza o allegati di mail di persone conosciute ma con testi inspiegabili o in qualche modo strani.

Contattare i sistemi informativi prima di procedere a qualsiasi attività potenzialmente in conflitto con quanto sopra.

GESTIONE INTERNET

1. Premessa

La connessione alla rete Internet dal device avuto in dotazione è ammessa esclusivamente per motivi attinenti allo svolgimento dell’attività lavorativa.
L’utilizzo per scopi personali è permesso con moderazione e con gli accorgimenti di cui al presente documento.
In particolare si vieta l’utilizzo dei social network, se non espressamente autorizzati.

2. 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 blacklist.

3. Divieti Espressi concernenti internet

1. È vietata la navigazione nei siti che possono rivelare le opinioni politiche religiose, sindacali e di salute dell’Incaricato poiché potenzialmente idonea a rivelare dati sensibili ai sensi del Codice Privacy.
2. È fatto divieto di accedere a siti Internet che abbiano un contenuto contrario a norme di legge e a norme a tutela dell’ordine pubblico, rilevante ai fini della realizzazione di una fattispecie di reato o che siano in qualche modo discriminatori sulla base della razza, dell’origine etnica, del colore della pelle, della fede religiosa, dell’età, del sesso, della cittadinanza, dello stato civile, degli handicap.
3. È vietato all’autorizzato lo scarico di software (anche gratuito) prelevato da siti Internet;
4. 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 dal Titolare e con il rispetto delle normali procedure di acquisto.
5. È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all’attività lavorativa.
6. È vietata la partecipazione a forum non professionali, l’utilizzo di chat line, di bacheche elettroniche o partecipare a gruppi di discussione o lasciare commenti ad articoli o iscriversi a mailing list spendendo il marchio o la denominazione dell’organizzazione, salvo specifica autorizzazione dell’organizzazione stessa.
7. È vietata la memorizzazione di documenti informatici di natura oltraggiosa, diffamatoria e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
8. È vietato all’Incaricato di promuovere utile o guadagno personale attraverso l’uso di Internet o della posta elettronica aziendale.
9. È vietato accedere dall’esterno alla rete interna dell’organizzazione, salvo con le specifiche procedure previste dall’ente stesso.
10. È vietato, infine, creare siti web personali sui sistemi dell’organizzazione nonché acquistare beni o servizi su Internet a meno che l’articolo acquistato non sia stato approvato a titolo di spesa professionale.

Ogni eventuale navigazione di questo tipo, comportando un illegittimo utilizzo di Internet, nonché un possibile illecito trattamento di dati personali e sensibili è posta sotto la personale responsabilità dell’Incaricato inadempiente.

4. Divieti di Sabotaggio

È vietato accedere ad alcuni siti Internet mediante azioni inibenti dei filtri, sabotando o comunque superando o tentando di superare o disabilitando i sistemi adottati dall’ente per bloccare accessi non conformi all’attività lavorativa. In ogni caso è vietato utilizzare siti o altri strumenti che realizzino tale fine.

5. Diritto d’autore

È vietato utilizzare l’accesso ad Internet in violazione delle norme in vigore nell’ordinamento giuridico italiano a tutela del diritto d’autore (es. legge 22 aprile 1941, n. 633 e successive modificazioni, d.lgs. 6 maggio 1999, n. 169 e legge 18 agosto 2000, n. 248). In particolare, è vietato il download di materiale soggetto a copyright (testi, immagini, musica, filmati, file in genere, …) se non espressamente autorizzato dall’organizzazione.

POSTA ELETTRONICA

1. Premessa

L’utilizzo della posta elettronica aziendale è connesso allo svolgimento dell’attività lavorativa.
L’uso per motivi personali deve essere moderato ed è tollerato esclusivamente ai sensi dell’articolo seguente.
Gli autorizzati possono avere in utilizzo indirizzi nominativi di posta elettronica.
Le caselle e-mail possono meglio essere assegnate con natura impersonale (tipo info, amministrazione, fornitori, direttore, direttore sanitario, consulenza, …) proprio per evitare ulteriormente che il destinatario delle mail possa considerare l’indirizzo assegnato al dipendente “privato”, ai sensi dei suggerimenti del Garante a tal proposito.
Gli autorizzati assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

2. Misure preventive per ridurre illeciti della Posta Elettronica

L’organizzazione è consapevole della possibilità di un limitato utilizzo personale della posta elettronica da parte degli autorizzati e allo scopo prevede le seguenti misure:

1. In caso di ricezione sulla e-mail aziendale di posta personale si avverte di cancellare immediatamente ogni messaggio al fine di evitare ogni eventuale e possibile backup dei dati.
2. Avvisare l’organizzazione quando alla propria posta personale siano allegati *files* eseguibili e/o di natura incomprensibile o non conosciuta.

3. Divieti Espressi

- È vietato utilizzare l’indirizzo di posta elettronica contenente il dominio dell’organizzazione per iscriversi in qualsivoglia sito per motivi non attinenti all’attività lavorativa, senza espressa autorizzazione scritta dell’organizzazione, nonché utilizzare il dominio dell’organizzazione per scopi personali.

- Quando si redigono messaggi di posta elettronica utilizzando l’indirizzo aziendale, diretti a destinatari esterni dell’organizzazione, è consigliabile utilizzare il seguente disclaimer:
  «Il presente messaggio e gli eventuali suoi allegati sono di natura aziendale, prevalentemente confidenziale e sono visionabili solo dal destinatario di posta elettronica. La risposta o l’eventuale invio spontaneo, da parte vostra, di e-mail al nostro indirizzo, potrebbero non assicurare la confidenzialità potendo essere viste da altri soggetti appartenenti all’organizzazione oltre al sottoscritto, per finalità di sicurezza informatica, amministrative e allo scopo del continuo svolgimento dell’attività aziendale. Qualora questo messaggio vi fosse pervenuto per errore, vi preghiamo di cancellarlo dal vostro sistema e vi chiediamo di volercene dare cortesemente comunicazione al mittente”.

- È vietato creare, archiviare o spedire, anche solo all’interno della rete aziendale, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) non connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto, “catene di Sant’Antonio” o in genere a pubblici dibattiti utilizzando l’indirizzo aziendale.

- È vietato trasmettere messaggi a gruppi numerosi di persone (es. a tutto un ufficio o ad un’intera divisione) senza l’autorizzazione necessaria.
- È vietato sollecitare donazioni di beneficenza, propaganda elettorale o altre voci non legate al lavoro.
- È vietato utilizzare il servizio di posta elettronica per trasmettere a soggetti esterni dell’organizzazione informazioni riservate o comunque documenti aziendali, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte.
- È vietato utilizzare la posta elettronica per messaggi con allegati di grandi dimensioni.

4. Posta Elettronica in caso di assenze programmate ad assenze non programmate

Nel caso di assenza prolungata sarebbe buona norma attivare il servizio di risposta automatica (*Auto-reply*).
In alternativa e in tutti i casi in cui sia necessario un presidio della casella di e-mail per ragioni di operatività aziendale, l’Incaricato deve nominare un collega fiduciario con lettera scritta che in caso di assenza inoltri i *files* 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 e redigendo apposito verbale.

5. Utilizzo Illecito di Posta Elettronica

1. È vietato inviare, tramite la posta elettronica, anche all’interno della rete aziendale, materiale a contenuto violento, sessuale o comunque offensivo dei principi di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico.
2. È vietato inviare messaggi di posta elettronica, anche all’interno della rete aziendale, che abbiano contenuti contrari a norme di legge ed a norme di tutela dell’ordine pubblico, rilevanti ai fini della realizzazione di una fattispecie di reato, o che siano in qualche modo discriminatori della razza, dell’origine etnica, del colore della pelle, della fede religiosa, dell’età, del sesso, della cittadinanza, dello stato civile, degli handicap.
3. Qualora l’Incaricato riceva messaggi aventi tale contenuto, è tenuto a cancellarli immediatamente e a darne comunicazione all’organizzazione.

GESTIONE DI ALTRI DEVICE (PERSONAL COMPUTER PORTATILE, TABLET, CELLULARE, SMARTPHONE E DI ALTRI DISPOSITIVI ELETTRONICI)

1. Utilizzo del notebook, tablet o smartphone

Il computer portatile, il tablet e il cellulare (di seguito generalizzati in “*device mobile*”) possono venire concessi in uso dall’organizzazione agli Incaricati che durante gli spostamenti necessitino di disporre di archivi elettronici, supporti di automazione e/o di connessione alla rete dell’organizzazione.
L’autorizzato è responsabile dei device mobili assegnatigli dall’organizzazione e deve custodirli con diligenza sia durante gli spostamenti sia durante l’utilizzo nel luogo di lavoro.
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 *files* 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’ente.
I device mobili utilizzati all’esterno (convegni, visite in azienda, ecc…), in caso di allontanamento, devono essere custoditi in un luogo protetto.
In caso di perdita o furto dei device mobili deve far seguito la denuncia alle autorità competenti. Allo scopo si deve avvisare immediatamente l’ente che provvederà – se del caso – ad occuparsi delle procedure connesse alla privacy. Anche di giorno, durante l’orario di lavoro, all’ autorizzato non è consentito lasciare incustoditi i device mobili.
All’autorizzato è vietato lasciare i device mobili incustoditi e a vista dentro l’auto o in una stanza d’albergo o 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) devono sempre essere abilitabili solo con la digitazione del PIN stesso e non possono essere lasciti privi di PIN.
Laddove il device mobile sia accompagnato da un’utenza, l’autorizzato è chiamato ad informarsi preventivamente dei vincoli ad essa associati (es. numero minuti massimo, totale gigabyte dati, …) e a rispettarli. Qualora esigenze lavorative richiedessero requirements differenti l’autorizzato è tenuto ad informare tempestivamente e preventivamente l’ente.
In relazione alle utenze mobili, salvo autorizzazione dell’organizzazione, è espressamente vietato ogni utilizzo all’estero e anche in caso di autorizzazione dell’organizzazione, gli utilizzi all’esterno devono essere preventivamente comunicati all’organizzazione per permettere l’attivazione di opportuni contratti di copertura con l’operatore mobile di riferimento.

2. Memorie esterne (chiavi usb, hard disk, memory card, cd-rom, dvd, ecc…)

Agli Incaricati può essere assegnata una memoria esterna (quale una chiave USB, un hard disk esterno, una memory card, …) su cui copiare temporaneamente dei dati per un facile trasporto, o altri usi (es. macchine fotografiche con memory card, videocamere con dvd, …).
Questi dispositivi devono essere gestiti con le stesse accortezze di cui all’articolo precedente e devono essere utilizzati esclusivamente dalle persone a cui sono state affidate e, in nessun caso, devono essere consegnate a terzi.

3. Divieti personali

Ai dipendenti non è permesso svolgere la loro attività su PC fissi, portatili, device personali.
Ai dipendenti, se espressamente autorizzati dall’ente, è permesso solo l’utilizzo della posta elettronica aziendale sui loro device personali.
In tal caso è necessario che il device abbia password di sicurezza stringenti approvate dall’ente e l’eventuale furto o smarrimento del device deve essere immediatamente segnalato anche all’ente 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, …).
Gli autorizzati non dipendenti (ovvero i consulenti e collaboratori esterni), possono utilizzare i propri device personali per memorizzare dati dell’ente solo se espressamente autorizzati dall’ente stesso e assumendone formalmente e personalmente l’intera responsabilità del trattamento.
Tali device dovranno essere preventivamente valutati dall’ente, per la verifica della sussistenza di misure minime ed idonee di sicurezza.

4. Utilizzo del Cellulare/smartphone personale

Durante l’orario di lavoro, comprese le eventuali pause, agli autorizzati è concesso l’utilizzo del telefono cellulare personale ma solo per comunicazioni di emergenza o strettamente collegate all’ambito lavorativo.
In caso di trasferte lavorative all’esterno degli uffici dell’organizzazione, il telefono personale può rimanere acceso, anche per facilitare la comunicazione con l’organizzazione stessa ove fosse necessario.
In questo caso si invita, comunque, a non utilizzarlo per fini personali, in modo particolare alla presenza di clienti o fornitori.
Gli Incaricati non dipendenti (ovvero i consulenti e collaboratori esterni), possono utilizzare i propri cellulari/smartphone per memorizzare dati dell’ente solo se espressamente autorizzati dall’ente stesso e assumendone formalmente e personalmente l’intera responsabilità del trattamento.
Tali cellulari/smartphone dovranno essere preventivamente valutati dall’ente, per la verifica della sussistenza di misure minime ed idonee di sicurezza.

5. 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 all’ente che provvederà a distruggerli o a ricondizionarli seguendo le norme di legge in vigore al momento.
In particolare l’ente provvederà a cancellare o a rendere inintelligibili.

GESTIONE SISTEMI IN CLOUD

1. Cloud Computing

In informatica con il termine inglese *cloud computing* (in italiano nuvola informatica) si indica un paradigma di erogazione di risorse informatiche, come l'archiviazione, l'elaborazione o la trasmissione di dati, caratterizzato dalla disponibilità on demand attraverso Internet a partire da un insieme di risorse preesistenti e configurabili.
Le risorse non vengono pienamente configurate e messe in opera dal fornitore apposta per l'utente, ma gli sono assegnate, rapidamente e convenientemente, grazie a procedure automatizzate, a partire da un insieme di risorse condivise con altri utenti lasciando all'utente parte dell'onere della configurazione. Quando l'utente rilascia la risorsa, essa viene similmente riconfigurata nello stato iniziale e rimessa a disposizione nel pool condiviso delle risorse, con altrettanta velocità ed economia per il fornitore.
Utilizzare un servizio di cloud computing per memorizzare dati personali o sensibili, espone l'ente a potenziali problemi di violazione della privacy. I dati personali vengono memorizzati nel server *farms* di aziende che spesso risiedono in uno stato diverso da quello dell'ente. Il cloud provider, in caso di comportamento scorretto o malevolo, potrebbe accedere ai dati personali per eseguire ricerche di mercato e profilazione degli utenti,
Con i collegamenti wireless, il rischio sicurezza aumenta e si è maggiormente esposti ai casi di pirateria informatica a causa della minore sicurezza offerta dalle reti senza fili. In presenza di atti illegali, come appropriazione indebita o illegale di dati personali, il danno potrebbe essere molto grave per l'ente, con difficoltà di raggiungere soluzioni giuridiche e/o rimborsi se il fornitore risiede in uno stato diverso da paese dell'utente.
Nel caso di industrie o aziende, tutti i dati memorizzati nelle memorie esterne sono seriamente esposti a eventuali casi di spionaggio industriale.

2. Utilizzo di sistemi cloud

È vietato agli autorizzati l’utilizzo di sistemi cloud non espressamente approvati dall’ente. Per essere approvati i sistemi cloud dovrebbero rispondere ad almeno i seguenti requisiti:

- Essere sistemi cloud esclusivi e non condivisi;
- Essere sistemi cloud posizionati fisicamente in Italia o in un paese europeo;
- L’azienda che fornisce il sistema in cloud deve essere preventivamente nominata Responsabile al Trattamento dei dati da parte dell’ente;
- L’azienda che fornisce il sistema in cloud deve comunicare all’ente, almeno una volta all’anno, i nominativi degli amministratori di sistema utilizzati.
- Dovranno essere verificate tutte le indicazioni e prescrizioni previste dal Garante della Privacy nei suoi provvedimenti sugli Amministratori di Sistema e sul cloud.

GESTIONE DATI CARTACEI

1. Clear Desk Policy

Gli Incaricati sono responsabili del controllo e della custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.
Gli Incaricati sono invitati dall’organizzazione ad adottare una “politica della scrivania pulita”. Ovvero si richiede agli incaricati di trattare dati cartacei solo se necessario, privilegiando, ove possibile, l’utilizzo degli strumenti digitali messi a disposizione dell’ente.

I principali benefici di una politica della scrivania pulita sono:

1) Una buona impressione a clienti e fornitori che visitano la nostra organizzazione;
2) La riduzione della possibilità che informazioni confidenziali possano essere viste da persone non abilitate a conoscerle;
3) La riduzione che documenti confidenziali possano essere sottratti all’organizzazione.

In particolare, si invita a non lasciare in vista sulla propria scrivania dati cartacei quando ci si allontana dalla stessa oppure quando è previsto un incontro con un soggetto non abilitato alla conoscenza dei dati in essi contenuti.
Prima di lasciare la propria postazione (per esempio per la pausa pranzo o per una riunione) sarà cura degli Incaricati riporre in luogo sicuro (armadio, cassettiera, archivio, …) i dati cartacei ad esso affidati, affinché gli stessi non possano essere visti da terzi non autorizzati (es. addetti alle pulizie) o da terzi (visitatori) presenti nell’ente.
A fine giornata deve essere previsto il riordino della scrivania e la corretta archiviazione di tutte le pratiche d’ufficio, in modo da lasciare la scrivania completamente sgombra.
Ove possibile, si invita ad evitare la stampa di documenti digitali, anche ai fini di ridurre l’inquinamento ed il consumo delle risorse in ottica ecologica.
Ove possibile, si invita ad effettuare la scansione dei documenti cartacei ed archiviarli digitalmente.
È necessario rimuovere immediatamente ogni foglio stampato da una stampante o da un’apparecchiatura fax, per evitare che siano prelevati o visionati da soggetti non autorizzati.
Ove possibile, è buona norma eliminare i documenti cartacei attraverso apparecchiature trita documenti.

RESTITUZIONE DEI DEVICE DELL’ENTE A SEGUITO DI CESSAZIONE DEL RAPPORTO DI LAVORO

Nel caso in cui il dipendente abbia possesso di device aziendali, utilizzati per i soli scopi lavorativi, al termine del rapporto di lavoro ha l’obbligo di restituirli.
A tal fine è posto in capo al lavoratore il divieto di distruggere, alterare e formattare gli strumenti, i quali verranno eventualmente ricondizionati dall’ente al fine di riconsegnarli privi di contenuti ad altro soggetto.
Prima del ricondizionamento provvederemo al vaglio dei dati contenuti sui device, in quanto proprietari degli stessi, in modo da effettuare l’immediata cancellazione delle informazioni non utili.
Le informazioni verranno conservate per 10 anni se di tipo amministrativo mentre è consigliabile per 3 anni con riguardo a tutti gli altri dati che potrebbero risultare utili per il corretto proseguo dell’attività (per esempio dati clienti, informazioni su prodotti ecc.).
Il salvataggio di questi dati avverrà a mezzo di backup su supporto dell’ente e conservato per il tempo sopraindicato.

PROVVEDIMENTI DISCIPLINARI

1. Conseguenza delle infrazioni disciplinari

Le infrazioni disciplinari alle norme del presente Disciplinare 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:

1. Il biasimo inflitto verbalmente;
2. Lettera di richiamo inflitto per iscritto;
3. Multa;
4. La sospensione dalla retribuzione e dal servizio;
5. 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’ente potrà procedere al licenziamento del dirigente autore dell’infrazione.

2. Modalità di Esercizio dei diritti

Il lavoratore interessato del trattamento dei dati effettuato mediante strumenti informatici ha diritto di accedere ai sensi degli artt. dal 15 al 21 del Regolamento Europeo UE 2016/679 alle informazioni che lo riguardano scrivendo al Titolare dell’organizzazione.

VALIDITA’

Il presente Disciplinare ha validità a partire da: _____(data)

AGGIORNAMENTO

Il presente Disciplinare 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 Disciplinare sarà comunicata agli autorizzati al trattamento dei dati.

AFFISSIONE

Il presente Disciplinare verrà affisso nella bacheca aziendale (se presente) e pubblicato sulla intranet aziendale ai sensi dell’art. 7 della legge 300/70 e del CCNL.

_____
Firma del Titolare o Responsabile del trattamento dei dati

Data _____

In data odierna il presente documento è stato consegnato a _____ (nome incaricato), che dichiara di averlo ricevuto e di averne preso visione.

_____
Firma dell’autorizzato