POLITICHE OPERATIVE:

- *REGOLAMENTO* "Formativo" in materia di Protezione dei Dati Personali – GDPR N. 679/16

Versione: 2021/2022
Materiale prodotto da ***PrivacyControl***

Dott. Massimo Zampetti
Partner I *Audit & Compliance*

POLITICHE OPERATIVE

II_A AMBITO GENERALE

Definizioni

D.Lgs. 196/2003*: Decreto Legislativo 196 del 30 giugno 2003 e sue successive modifiche ed integrazioni;*

Regolamento Europeo 679/2016: *Regolamento europeo 2016/679 del Parlamento Europeo del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);*

D.Lgs. 101/2018*: Decreto Legislativo 101 del 19 settembre 2018, attuativo del GDPR 679/18, modica il D.Lgs. 196/03;*

NDA*: non-disclosure agreement, ovvero accordo di non divulgazione, è un negozio giuridico di natura sinallagmatica che designa informazioni confidenziali e con il quale le parti si impegnano a mantenerle segrete, pena la violazione dell'accordo stesso e il decorso di specifiche clausole penali in esso contenute.;*

Dipendente*: personale dell'ente assunto con qualsiasi tipo di forma contrattuale, anche in stage o tirocinio;*

Incaricato/Designato*: ogni dipendente, come sopra identificato, ed ogni consulente esterno che, nell'ambito dell'attività assegnatagli, tratta dati (nell'accezione del capitolo seguente) riferiti all'ente.*

POLITICHE PRIVACY in materia di GDPR N. 679/16

Premessa

La nostra organizzazione gestisce 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 679/2016 e del D.lgs. 101/2018 e s.m.i., "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 dell'organizzazione.
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 dell'organizzazione 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 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 dell'organizzazione, 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 degli articoli 13-14 del Regolamento Europeo 679/2016 e costituiscono, quindi, parte integrante dell'informativa rilasciata agli Incaricati.
L'inosservanza delle norme sulla privacy può comportare sanzioni di natura civile e penale per l'incaricato e per l'Ente per cui si raccomanda di prestare la massima attenzione nella lettura delle disposizioni di seguito riportate.

Esclusione all'uso degli strumenti informatici

All'inizio del rapporto lavorativo o di consulenza, l'ente valuta la presenza dei presupposti per l'autorizzazione all'uso dei vari device dell'Ente, di internet e della posta elettronica da parte degli incaricati.
Successivamente e periodicamente l'ente valuta la permanenza dei presupposti per l'utilizzo dei device dell'Ente, di internet e della posta elettronica.
È fatto esplicito divieto ai soggetti non autorizzati di accedere agli strumenti informatici dell'Ente.
I casi di esclusione possono riguardare:

1. *L'utilizzo del COMPUTER o di altri DEVICE;*
2. *L'utilizzo della posta elettronica;*
3. *L'accesso a internet.*

Le eventuali esclusioni sono strettamente connesse al principio della natura dell'organizzazione e lavorativa degli strumenti informatici nonché al principio di necessità di cui al Nuovo Codice Privacy e Regolamento Europeo 679/2016. Più specificatamente hanno diritto all'utilizzo degli strumenti e ai relativi accessi solo gli incaricati che, per funzioni lavorative, ne abbiano un effettivo e concreto bisogno.
I casi in cui le esclusioni dovranno risultare operative in forza di tali motivazioni verranno comunicati individualmente e potranno riguardare sia tutti i casi sopra descritti, sia solo uno o due degli stessi.
Si informa che tali esclusioni sono divenute necessarie alla luce del Provvedimento del Garante 1° marzo 2007 che indica di ridurre a titolo cautelativo e preventivo l'utilizzo degli strumenti informatici in considerazione dei pericoli e delle minacce indicate in questo documento.

Titolarità degli strumenti elettronici e dei dati

L'organizzazione è esclusiva titolare e proprietaria degli strumenti elettronici messi a disposizione degli Incaricati ai soli fini dell'attività lavorativa.
L'ente è l'unica esclusiva titolare e proprietaria di tutte le informazioni, le registrazioni ed i dati contenuti e/o trattati mediante i propri device digitali o archiviati in modo cartaceo nei propri locali.
L'incaricato non può presumere o ritenere che le informazioni, le registrazioni ed i dati da lui trattati o memorizzati negli strumenti elettronici dell'Ente (inclusi i messaggi di posta elettronica e/o chat inviati o ricevuti, i file di immagini, i file di filmati o altre tipologie di file) siano privati o personali, né può presumere che dati cartacei in suo possesso possano essere da lui copiati, comunicati o diffusi senza l'autorizzazione dell'organizzazione.

Finalità nell'utilizzo dei device

I device assegnati sono uno strumento lavorativo nelle disponibilità dell'incaricato esclusivamente per un fine di carattere lavorativo. I device, quindi, non devono essere utilizzati per finalità private e diverse da quelle dell'Ente, se non eccezionalmente e nei limiti evidenziati dal presente Disciplinare. Qualsiasi eventuale tolleranza da parte di questo ente, apparente o effettiva, non potrà, comunque, legittimare comportamenti contrari alle istruzioni contenute nel presente Disciplinare.

Restituzione dei device

A seguito di una cessazione del rapporto lavorativo o di consulenza dell'incaricato con l'organizzazione o, comunque, al venir meno, ad insindacabile giudizio dell'ente, della permanenza dei presupposti per l'utilizzo dei device dell'Ente, gli incaricati hanno i seguenti obblighi:

1. Procedere immediatamente alla restituzione dei device in uso;

2. Divieto assoluto di formattare o alterare o manomettere o distruggere i device assegnati o rendere inintelligibili i dati in essi contenuti tramite qualsiasi processo.

Restituzione dei dati cartacei

A seguito di una cessazione del rapporto lavorativo o di consulenza dell'incaricato con l'organizzazione o, comunque, al venir meno, ad insindacabile giudizio dell'ente, della permanenza dei presupposti per l'utilizzo di dati cartacei dell'Ente, gli incaricati hanno i seguenti obblighi:

1. *Procedere immediatamente alla restituzione dei dati cartacei in loro possesso;*
2. *Divieto assoluto di alterare o manomettere o distruggere i dati cartacei assegnati o renderli inintelligibili tramite qualsiasi processo.*

II_B PASSWORD

Le Password

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, e 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.
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 verranno 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.

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 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;
6. Evitare di digitare la propria password in presenza di altri soggetti che possano vedere la tastiera, anche se collaboratori o dipendenti dell'ente.

Divieto di uso

Al fine di una corretta gestione delle password, l'organizzazione stabilisce il divieto di utilizzare 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 (in particolare data di nascita propria o di persone vicine, o di altre importanti ricorrenze), mesi dell'anno e giorni della settimana, anche in lingua straniera;
6. Parole banali e/o di facile intuizione;
7. Ripetizioni di sequenze di caratteri (es. abcabcabc);
8. Una password già impiegata in precedenza.

La password nei sistemi

Ogni incaricato può variare la propria password di accesso a qualsiasi sistema dell'organizzazione in modo autonomo, qualora il sistema in questione metta a disposizione degli Utenti una funzionalità di questo tipo oppure facendone richiesta al titolare. La password può essere sostituita dal titolare, anche qualora l'Utente l'abbia dimenticata.

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.

II_C OPERAZIONI A PROTEZIONE DELLA POSTAZIONE DI LAVORO

Login e Logout

Il "Login" è l'operazione con la quale l'incaricato si connette al sistema informativo dell'organizzazione 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.

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 dell'organizzazione.
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.

II_D USO DEL PERSONAL COMPUTER DELL'ENTE

Modalità d'uso del COMPUTER dell'organizzazione

Il sistema informativo dell'organizzazione è composto da un insieme di macchine client, che utilizzano diversi sistemi operativi e applicativi.
I file creati, elaborati o modificati sul computer assegnato devono essere poi sempre salvati a fine giornata.
L'Ente effettua il backup dei dati memorizzati in locale su dispositivo USB esterno.

Corretto utilizzo del COMPUTER dell'organizzazione

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.
L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato 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 dell'Ente, 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 alle memorie di massa locali di rete (repository e backup) che ai server dell'Ente nonché, previa comunicazione al dipendente, accedere al computer, anche in remoto.
In particolare, l'incaricato 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 file 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.

Divieti Espressi sull'utilizzo del COMPUTER

All'incaricato è vietato:
1. La gestione, la memorizzazione (anche temporanea) o il trattamento di file, documenti e/o informazioni personali dell'incaricato o comunque non afferenti alle attività lavorative nella rete, nel disco fisso o in altre memorie di massa dell'Ente e negli strumenti informatici dell'Ente 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, PCMCIA, 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 dall'Ente.

ANTIVIRUS

I virus possono essere trasmessi tramite scambio di file via internet, via mail, scambio di supporti removibili, file-sharing, chat, via mail, ecc... 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'incaricato, 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 dell'organizzazione senza servizio antivirus attivo e aggiornato sulla propria postazione;
2. È vietato ostacolare l'azione dell'antivirus dell'organizzazione;
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.

II_E INTERNET

Internet: uno strumento di lavoro

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.

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.

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 Nuovo Codice Privacy e del Regolamento Europeo 679/2016.
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'incaricato 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 dell'organizzazione.
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.

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 realizzinotale fine.

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.

II_F POSTA ELETTRONICA

La Posta Elettronica è uno strumento di lavoro

L'utilizzo della posta elettronica dell'organizzazione 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 Incaricati 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 Incaricati assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

Misure Preventive per ridurre utilizzi illeciti della Posta Elettronica

L'organizzazione è consapevole della possibilità di un limitato utilizzo personale della posta elettronica da parte degli Incaricati e allo scopo prevede le seguenti misure:
1. In caso di ricezione sulla e-mail dell'organizzazione di posta personale si avverte di cancellare immediatamente ogni messaggio al fine di evitare ogni eventuale e possibile back up dei dati.
2. Avvisare l'organizzazione quando alla propria posta personale siano allegati file eseguibili e/o di natura incomprensibile o non conosciuta.

Divieti Espressi

1. 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.
2. È vietato redigere messaggi di posta elettronica utilizzando l'indirizzo dell'organizzazione, diretti a destinatari esterni dell'organizzazione, senza utilizzare il seguente disclaimer:
«Il presente messaggio e gli eventuali suoi allegati sono di natura privata collegata all'organizzazione, 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 lavorativa. 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".
3. È vietato creare, archiviare o spedire, anche solo all'interno della rete dell'organizzazione, 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 personale collegato all'organizzazione.
4. È vietato trasmettere messaggi a gruppi numerosi di persone (es. a tutto un ufficio o ad un'intera divisione) senza l'autorizzazione necessaria.

5. È vietato sollecitare donazioni di beneficenza, propaganda elettorale o altre voci non legate al lavoro.
6. È vietato utilizzare il servizio di posta elettronica per trasmettere a soggetti esterni dell'organizzazione informazioni riservate o comunque documenti dell'Ente, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte.
7. È vietato utilizzare la posta elettronica per messaggi con allegati di grandi dimensioni.

Posta Elettronica in caso di assenze programmate ed 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 dell'organizzazione, l'incaricato deve nominare un collega fiduciario con lettera scritta 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 e redigendo apposito verbale.

Utilizzo Illecito di Posta Elettronica

1. È vietato inviare, tramite la posta elettronica, anche all'interno della rete dell'organizzazione, materiale a contenuto violento, sessuale o comunque offensivo dei principî 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 dell'organizzazione, 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.

II_G GESTIONE DATI CARTACEI

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 agli interessati e ai 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.

II_H GESTIONE INCIDENTE DI SICUREZZA DELLE INFORMAZIONI

L'obiettivo è quello di garantire che l'impresa reagisca in modo appropriato a qualsiasi tipologia, effettiva o presunta, di incidenti di sicurezza relativamente ai sistemi informativi e ai dati.
L'Ente ha la responsabilità di monitorare tutti gli incidenti che si verificano al suo interno che possono violare la sicurezza e/o la riservatezza delle informazioni. Tutti gli incidenti devono essere identificati, segnalati, studiati e monitorati: lo scopo principale di questa politica non è quello di attribuire colpe, ma di contenere i problemi e apprendere dagli errori in ottica di miglioramento continuo.

Modalità operative

Partiamo dalla definizione: con "incidenti di sicurezza delle informazioni" s'intende un evento avverso che ha causato o ha il potenziale di causare danni agli assets, alla reputazione e/o al personale dell'organizzazione, attraverso l'intrusione, la compromissione e l'abuso di informazioni e risorse. Quindi è la realizzazione di una delle minacce analizzate nel Risk Assessment dell'organizzazione.

Tipi di Incidenti
Le principali categorie di incidente sono:

- Incidenti **CRITICI** devono essere segnalati immediatamente
  Es.
  - furto di documenti
  - computer infettato da virus
- Incidenti **SIGNIFICATIVI** devono essere segnalati entro 4 ore
  Es.
  - uso di un software privo di licenza
  - accesso e/o uso non autorizzato dei dati di accesso di un altro utente
- Incidenti **MINORI** devono essere segnalati entro 1 giorno
  Es.
  - Tentata penetrazione delle difese
  - Spedizioni email non appropriate

Rischi
L'organizzazione riconosce che ci sono dei rischi associati all'accesso degli utenti e alla gestione delle informazioni nello svolgimento delle proprie attività, infatti questa politica mira a:

- ✓ Ridurre l'impatto delle violazioni di sicurezza, assicurando che gli incidenti siano seguiti correttamente.
- ✓ Aiutare a identificare le aree di miglioramento per ridurre il rischio e l'impatto di futuri incidenti.
- ✓ Ridurre il numero degli incidenti

Non conformità con questa politica potrebbe avere un impatto significativo sull'efficienza del funzionamento dell'organizzazione e può causare perdite finanziarie, multe e l'impossibilità di fornire i servizi necessari ai nostri clienti.

Procedura da seguire

Fase 1 **RILEVAZIONE INCIDENTE**

Un incidente può e deve essere rilevato:

- ✓ Dal personale operativo nello svolgimento delle proprie attività.
- ✓ Dall'avviso automatico dei dispositivi che monitorano le proprie attività di sistema.
- ✓ Dall' utente finale.

Fase 2 **VALUTAZIONE INCIDENTE**

Lo scopo di questa fase è quello di determinare rapidamente e con precisione se l'incidente è un incidente grave.

- ✓ Raccolta dati del problema iniziale - I dati sono raccolti e viene fatta un'appropriata classificazione dell'Impatto.
- ✓ Valutazione dell'Incidente - l'incidente è valutato e la relativa categoria è confermata dal Responsabile della Sicurezza delle informazioni.
- ✓ Incidente Grave - Se l'incidente è classificato come 'Critico', la valutazione deve essere confermata entro 60 minuti dalla rilevazione.

Fase 3 **COMUNICAZIONE INCIDENTE**

I processi di comunicazione hanno lo scopo di garantire che tutte le parti siano informate dello stato dell'incidente.

- ✓ I Responsabili di progetto e/o le parti coinvolte devono essere informati dell'incidente e tenuti aggiornati sui relativi progressi per consentire loro di gestire i propri clienti.
- ✓ In casi di incidente grave la Direzione deve essere informata e tenuta aggiornata.
- ✓ Qualora la violazione possa comportare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare di trattamento notifica al Garante entro 72h dal momento in cui ne è venuto a conoscenza. (Vedi *Modulo Segnalazione Data Breach*).

Fase 4 **RISOLUZIONE INCIDENTE**

Questa fase comprende tutte le varie indagini tecniche che saranno necessarie per portare l'incidente a risoluzione; può richiedere l'intervento di diverse figure tecniche e non – si prevede che le risorse siano rese disponibili su richiesta.

Fase 5 **POST-RISOLUZIONE INCIDENTE**

Il processo di post-risoluzione è avviato una volta che l'incidente è stato risolto.

⇒ *Riesame Incidente Critico*: Il Responsabile della Sicurezza delle Informazioni, in occasione di incidente grave, indice una riunione di riesame entro 3 giorni lavorativi dalla data di risoluzione dell'incidente, alla quale partecipa il personale coinvolto.

⇒ *Verbale Incidente Critico*: E' costituito dal verbale della riunione di riesame: riassume gli eventi dell'incidente, l'impatto, le azioni intraprese per risolvere l'incidente e le ulteriori misure adottate per ridurre il rischio di accadimento futuro/impatto.

⇒ *Incidente Non Critico*: E' segnalato tramite la compilazione di un verbale.