Regole di base per l'utilizzo Dei sitemi informativi

Data: 02/07/2019	FILE: Nuova privacy 679.2016.docx	
Manuale Rev.02	Relatore: DIPARTIMENTO IT TREVI	

Indice

Generalità

Il presente documento indica le norme generali e di buon senso per il corretto impiego delle informazioni presenti – a qualsiasi titolo – all'interno della **SITEM S.p.A.**; si tratta cioè di un insieme di norme comportamentali e regole pratiche atte a prevenire danneggiamento, distruzione, alterazione o perdita di accessibilità ai dati aziendali.

Con il termine "sicurezza" ci si riferisce a tre aspetti distinti:

⇒ *Riservatezza**: prevenzione contro l'accesso non autorizzato alle informazioni;***
⇒ *Integrità**: le informazioni non devono alterabili da incidenti o abusi;***
⇒ *Disponibilità**: il sistema deve essere protetto da interruzioni impreviste.***

1.0 Norme di carattere generale per gli utenti che utilizzano strumenti informatici

- Trattare unicamente i dati relativi alle attività lavorative assegnate
- Non comunicare mai le informazioni desunte da documenti, archivi, ecc. se non autorizzati
- Non comunicare i dati trattati a colleghi che non abbiano l'esigenza di conoscerli per motivi di servizio
- Mettere in opera tutte le cautele possibili per evitare il danneggiamento e/o la perdita dei dati trattati, in base alle regole applicate da **SITEM S.p.A.** stessa
- Utilizzare gli appositi contenitori e quanto altro messo a disposizione dall'Azienda in caso di eliminazione di documenti cartacei contenenti le informazioni trattate
- Non effettuare copia non autorizzata dei dati
- Non conservare copie dei dati quando non sono più necessarie
- Rispettare eventuali procedure di applicazione del GDPR reg.EU 679/2016 comunicate dai clienti.

2.0 Custodia dei documenti cartacei

I documenti trattati dovranno essere soltanto quelli pertinenti alla propria mansione aziendale, in base alle indicazioni impartite dal proprio responsabile ed alle linee guida generali ricevute nella propria lettera di incarico.

2.1 Trattate e archiviate con cura i documenti

I dati cartacei devono essere conservati in faldoni, raccoglitori e cartelline, riposti negli appositi armadi, ove necessario muniti di ante con serratura, sugli scaffali e sulle scrivanie.

I documenti contenenti dati sensibili devono essere conservati in armadi chiusi a chiave, o – in alternativa – negli archivi che in azienda sono ad accesso selezionato e controllato.
Occorre ridurre al minimo la permanenza di documenti sulle proprie scrivanie. Nel caso di spostamenti in azienda con documenti riservati, impiegare sempre una cartellina o un raccoglitore non trasparente.

2.2 Maneggiate con cura le stampe di documenti riservati

Non lasciate accedere alle stampe persone non autorizzate; se la stampante non si trova sulla vostra scrivania recatevi quanto prima a ritirare le stampe. Distruggete personalmente le stampe quando non servono più.

2.3 Non gettate nel cestino le stampe di documenti che potrebbero contenere dati confidenziali

I documenti riservati che non servono più vanno opportunamente distrutti, e non cestinati.

2.4 Non effettuate copie o trascrizioni

Se non è necessario, e soprattutto se non si è autorizzati, non effettuare fotocopie o trascrizioni di stampe, tabulati, elenchi, rubriche e di ogni altro materiale. Inoltre, non consegnare a persone non autorizzate stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

2.5 Chiavi e badge

Le modalità di accesso e di utilizzo delle chiavi degli uffici o dei badge, degli archivi e degli armadi provvisti di chiavi sono stabilite dai rispettivi responsabili di funzione che provvedono, a loro discrezione, a comunicarle, anche verbalmente, a tutti o solo a qualcuno degli incaricati.

2.6 Divieto di portare documenti e dati fuori dall'

È di fatto vietato portare dati fuori dall'azienda e/o cederli a terzi, se non autorizzati.

2.7 Sicurezza e prevenzione

Rispettare sempre tutte le norme di sicurezza e prevenzione previste dalle procedure di sicurezza della **SITEM S.p.A.**

3.0 Sicurezza informatica

Il raggiungimento degli obbiettivi di sicurezza informatica si ottiene non solo con l'utilizzo di appropriati strumenti tecnologici, ma anche attraverso corretti comportamenti degli utenti. Infatti qualsiasi misura tecnica, per quanto possa essere sofisticata, non sarà pienamente efficace se non usata propriamente.

In particolare, le precauzioni di tipo tecnico possono proteggere le informazioni durante il loro transito attraverso i sistemi, o anche quando queste rimangono inutilizzate su un disco di un computer; nel momento in cui esse raggiungono l'utente finale, la loro protezione dipende esclusivamente da quest'ultimo, e nessuno strumento tecnologico può sostituirsi al suo senso di responsabilità e al rispetto delle norme.

3.1 Spegnete o bloccate sempre il vostro computer quando vi assentate dall'ufficio per un

lungo periodo

Lasciare un computer acceso non crea problemi al suo funzionamento, e al contrario velocizza il successivo accesso; tuttavia, un computer acceso è in linea di principio raggiungibile tramite la rete o anche direttamente sulla postazione di lavoro. Inoltre, più lungo è il periodo di assenza maggiore è la probabilità che un'interruzione dell'energia elettrica possa portare un danno. Per assenze più brevi, bloccare il sistema con <CTRL>+<ALT>+<CANC>, poi dare invio o fare click sul pulsante "Blocca Workstation".

3.2 Non lasciate lavori incompiuti sullo schermo

Chiudete sempre il programma quando vi allontanate dal posto di lavoro: potreste rimanere lontani più del previsto, e un documento presente sullo schermo è vulnerabile (quasi) quanto uno stampato o copiato su dischetto.

3.3 Non fate copie non autorizzate

Se non si è espressamente autorizzati, non effettuare copie su supporti magnetici o trasmissioni di dati. In caso di dubbio, fare sempre riferimento al proprio referente funzionale.

3.4 Conservate i supporti di memorizzazione in un luogo sicuro

A tutti i supporti di memorizzazione si applicano gli stessi criteri dei documenti cartacei, con l'ulteriore pericolo che il loro smarrimento (che può anche essere dovuto a un furto) può passare più facilmente inosservato. Di norma tutti i supporti devono essere affidati ai responsabili (coordinatore della sicurezza e amministratore di sistema); vanno quindi restituiti non appena finito di utilizzarli.

3.5 Prestate attenzione nell'affidare a terzi i vostri dati

Quando rimuovete un file, i dati non vengono effettivamente cancellati ma soltanto marcati come non utilizzati, e sono facilmente recuperabili. Neanche la formattazione assicura l'eliminazione dei vostri dati; solo l'utilizzo di un programma apposito garantisce che sul dischetto non resti traccia dei dati precedenti. Nel dubbio, è sempre meglio usare un supporto nuovo.

3.6 Riservatezza dei codici di accesso

Gli utenti possono aver a disposizione strumenti informatici e/o applicativi che necessitano di password per l'accesso. Le password devono soddisfare ad una serie di regole (impostate nei server) per garantire un sufficiente grado di protezione, e vanno cambiate tassativamente ogni tre oppure sei mesi, in base alle istruzioni impartite, o qualora l'utente sospetti anche una violazione del proprio account.

Anche se i programmi non ripetono in chiaro la password sullo schermo, quando digitate la vostra password questa potrebbe essere letta guardando i tasti che state battendo anche se avete buone capacità di dattiloscrittura. Le credenziali di accesso non vanno comunicate mai a nessuno – per nessun motivo – né in forma verbale né in forma scritta.
Le password non vanno scritte, meno che mai vicino alla postazione o in un file nel PC o nei server di rete. Ovunque possibile vanno imparate a memoria.

3.7 Formato delle password

Vanno usate password difficili da indovinare. Più avanti vedremo in maggior dettaglio come scegliere una password; in linea di massima, una sigla non banale è preferibile a una parola.

3.8 Unicità delle credenziali di accesso

Le credenziali di accesso sono personali e uniche. Non vanno comunicate né fatte usare a nessun'altra persona.

3.9 Non utilizzate le risorse se non per scopi di lavoro

L'utilizzo del proprio personal computer, dei server e delle risorse aziendali deve essere strettamente riservato alle attività di lavoro. In particolare, quindi, anche la posta elettronica e la navigazione in Internet devono essere assolutamente limitate all'impiego per finalità lavorative.

3.10 Non utilizzate apparecchi non autorizzati

L'utilizzo di modem su postazioni di lavoro collegati alla rete di edificio offre una porta d'accesso dall'esterno non solo al vostro computer, ma a tutta la Rete, ed è quindi assolutamente vietato, salvo autorizzazione scritta del responsabile Sitem.

3.11 Non installate programmi non autorizzati

Oltre alla possibilità di trasferire involontariamente un virus, va ricordato che la maggior parte dei programmi sono protetti da copyright, per cui la loro installazione può essere illegale. Inoltre programmi non contaminati, ma non autorizzati e valicati, possono comunque provocare danni al sistema, alla rete e ai dati aziendali.

3.12 Prevenzione dai software maligni

Nella sezione successiva vedremo in maggior dettaglio a quali aspetti bisogna prestare attenzione per proteggersi dai virus; in linea di massima, diffidate di tutti i dati e programmi che vi vengono consegnati, anche se la fonte appare affidabile.
La prevenzione dalle infezioni da virus sul vostro computer è molto più facile e comporta uno spreco di tempo molto minore della correzione degli effetti di un virus; tra l'altro, potreste incorrere in una perdita irreparabile di dati.

3.13 Salvataggio dei dati

Molti programmi applicativi, ad esempio quelli di videoscrittura, salvano automaticamente il lavoro a intervalli fissi, in modo da minimizzare il rischio di perdita accidentale dei dati. Imparate comunque a salvare manualmente il vostro lavoro con una certa frequenza, in modo da prendere l'abitudine di gestire voi stessi i dati e non fare esclusivo affidamento sul sistema.

Con la ristrutturazione della rete aziendale, avvenuta a fine 2017 abbiamo apportato alcune migliorie sulla sicurezza e sulle autorizzazioni alle cartelle di rete.
Struttura e procedure sono riportate in dettaglio nell'allegato **"FS-1 - struttura cartelle di rete e autorizzazioni cartelle"**

3.14 Politica dei backup

I dati delle applicazioni sono gestiti dai server, i file di lavoro delle applicazioni "office" devono essere salvati nel "*file server SITEM FS 10.99.1.11", nelle apposite cartelle messe a disposizione per ogni utente.* Qualsiasi file memorizzato nel proprio PC non è sicuro, e non viene salvato da

nessuno. Eccezione fatta per la posta elettronica, che risiede in parte in cloud nel provider gmail, e in parte nei pc degli utenti, e viene comunque salvata secondo accordi con i singoli utenti.

4.0 Protezione dai virus informatici

Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi. Alcuni virus si limitano a riprodursi senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido. Tutti i vostri sistemi sono dotati di Antivirus (se non lo fosse potete segnalarlo all'IT che provvederà ad installare il servizio). È vietato disabilitare l'antivirus.

COME SI TRASMETTE UN VIRUS:

- Attraverso programmi provenienti da fonti non ufficiali;
- Su internet, tramite browser (chrome, edge, internet explorer, firefox, ecc.);
- Attraverso la posta elettronica, soprattutto da messaggi di provenienza incerta;
- Attraverso supporti di memorizzazione quali usb key, floppy, CD-ROM, DVD, ecc.
- Attraverso file scambiati via rete;
- Attraverso le macro dei programmi di automazione d'ufficio (macro di word o excel).

COME NON SI TRASMETTE UN VIRUS:

- Attraverso mail in **formato testo** non contenenti allegati.

QUALI EFFETTI HA UN VIRUS?

- Lo spazio disco residuo si riduce inspiegabilmente;
- Le prestazioni del computer degradano parecchio o questo diventa inutilizzabile;
- Le informazioni registrate sono modificate o distrutte;
- Le informazioni del nostro PC o della nostra rete vengono trasmesse ad altri a nostra insaputa;
- Il nostro sistema viene usato come sponda per attaccare o offendere altri sistemi.

QUANDO SI SOSPETTA UNA INFEZIONE:

- Spegnete immediatamente il computer in modo da prevenire un maggior danno;
- Scrivete che cosa è successo e quali sono state le ultime azioni intraprese prima di accertare la presenza del virus in modo da aiutare gli esperti nelle successive azioni da intraprendere per rimuoverlo;
- Contattate sempre l'amministratore di sistema, anche se non siete sicuri che si tratti di un virus;

- Avvisate tutti coloro che ritenete possano essere stati infettati dallo stesso virus.

COME PREVENIRE I VIRUS:

- **Usate soltanto programmi autorizzati dall'azienda**
  Copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato.
- **Non usate giochi**
  L'impiego delle risorse deve essere strettamente limitato alle attività lavorative.
- **evitate i supporti esterni**
- Effettuare un attento controllo della posta elettronica. Ad oggi, la maggior parte dei virus si propagano ormai attraverso email fasulle (anche da PEC). È opportuno quindi prestare particolare attenzione a mittenti che non si conoscono.
- **Non partecipate a "catene di S. Antonio" e simili**
  Analogamente, tutti i messaggi che vi invitano a "diffondere la notizia quanto più possibile" sono bufale. Queste attività sono vietate dagli standard di Internet e contribuire alla loro diffusione. Sicuramente diffonde il nostro indirizzo di posta elettronica.

4.1 Impiego delle applicazioni

Le norme di prevenzione di base che gli utilizzatori dovranno seguire sono le seguenti:

- **Web browser e internet**
  - Non navigare in internet in siti non pertinenti con le proprie mansioni o comunque con finalità diverse da quelle degli obiettivi affidati dalla direzione
  - In ogni caso, non scaricare file e programmi senza l'autorizzazione del proprio responsabile di funzione o – per i programmi - dell'amministratore di sistema
- **Posta elettronica**
  - Non aprire messaggi eMail di dubbia provenienza, e comunque non aprire mai allegati dei quali non si conosca con certezza la provenienza e la finalità. In caso di necessità, effettuare una scansione del singolo file **prima** di aprirlo
  - Non utilizzare la finestra di anteprima messaggi nel client di posta elettronica
- **Regole varie**
  - Non impiegare supporti esterni (chiavette usb/cdrom/dvd) non necessari per la propria attività, e comunque diffidare di tutti quelli di dubbia provenienza

- Non installare mai software se non espressamente autorizzati dall'amministratore di sistema o dal coordinatore della sicurezza informatica

Come scegliere una password

Il più semplice metodo per l'accesso illecito a un sistema consiste nell'indovinare la password dell'utente legittimo. In molti casi sono stati procurati seri danni al sistema informativo a causa di un accesso protetto da password "deboli". La scelta di password difficile da indovinare è quindi, parte essenziale della sicurezza informatica.

È opportuno cambiare la password a intervalli regolari (almeno una volta l'anno). Usare password lunghe almeno sei caratteri composte da Lettere maiuscole e minuscole, numeri e simboli. Evitate di usare password che possano in qualche modo essere legate a Voi come, ad esempio, il Vostro nome, quello di Vostra moglie/marito, dei figli, del cane, date di nascita, numeri di telefono etc.