FASCICOLO INFORMATIVO SULL'USO DEL SISTEMA INFORMATICO AZIENDALE

1. Scopo del documento

Il presente documento illustra le linee guida per l'utilizzo del Sistema Informativo Aziendale (in breve SIA) del VI Circolo. La loro osservanza consente un corretto utilizzo del sistema informativo (in modo efficace, efficiente, etico e legale) in ottemperanza alle vigenti disposizioni di legge.

I fruitori di questo documento sono tutti gli utilizzatori del SIA, ovvero le persone autorizzate direttamente dal Dirigente al trattamento dei dati memorizzati nel SIA.

2. Definizioni

Con il termine "Sistema Informativo Aziendale" si intende un insieme di strumenti hardware (computer, server, reti di proprietà e di gestione) e software (sistemi operativi, applicativi e basi di dati) a cura del VI Circolo.

L'utilizzo del SIA include l'uso di dati o programmi memorizzati nei Sistemi Informatici, oppure l'uso di dati o programmi memorizzati su floppy, hard disk, CD-ROM o altri supporti di proprietà o di gestione.

L'utente del SIA è una persona autorizzata dal VI Circolo a cui è assegnato un account sul SIA per effettuare attività di trattamento dei dati per lo svolgimento delle attività di business specificate nello Statuto Aziendale.

3. Criticità della presente regolamentazione

Il "valore" dei Sistemi Informativi Aziendali, nella sua accezione più ampia di insieme di hardware, software di base, software applicativo e dati, nonché di impegno di risorse umane per la manutenzione, è tale da richiedere un'attenzione del tutto particolare da parte sia dei personale addetto al Settore Sistemi Informativi, che di tutto il personale utilizzatore dei Sistemi Informativi Aziendali.

L' attenzione è richiesta, e dovuta, per i seguenti motivi:

- delicatezza degli strumenti, procedure e dati utilizzati.
- necessità di assicurare una elevata affidabilità dei sistemi, in relazione alla rilevanza di tale aspetto per la funzionalità ed efficienza dei processi aziendali.

Il fine ultimo di un siffatto livello di gestione, è quello di garantire un'adeguata tutela del patrimonio dati presente nel SIA.

Le norme predisposte dal presente documento vanno intese come linee guida per la gestione/utilizzazione quotidiana del SIA. La mancata osservanza delle stesse può configurare una serie di ipotesi di reato in vari ambiti applicativi.

4. Utenti del SIA

Si distinguono due categorie di utenti: utenti non privilegiati, che hanno accesso ai soli dati e programmi a cui sono autorizzati, e utenti privilegiati, che hanno funzioni di amministrazione del sistema.

Il login come utente privilegiato deve essere limitato ai casi di effettiva necessità e per il solo periodo di tempo necessario a svolgere i compiti.

In tutti gli altri casi va utilizzato l'account non privilegiato.

5. Ruolo di amministratore di sistema

Il ruolo di Amministratore di Rete prevede, nei riguardi degli utilizzatori del SIA, l'assegnazione degli account, la verifica della permanenza delle condizioni di validità degli stessi ed il mantenimento dell'integrità degli account nel tempo.

6. Custode delle parole chiave

Nello specifico, il custode delle parole chiave dovrà ricevere da tutti gli utenti in busta chiusa la variazione della password, prevista almeno trimestralmente.

Il custode delle parole chiave, custodirà scrupolosamente le buste contenenti le password degli incaricati in luogo definito, ed utilizzerà la password necessaria, solamente in caso di assoluta necessità informando tempestivamente l'incaricato dell'intervento effettuato.

7. Accesso al SIA

L'accesso al SIA inteso come "patrimonio informatico" disponibile presso il VI Circolo è consentito ai dipendenti aziendali, in relazione alle proprie funzioni o competenze.

L'accesso al SIA è consentito solo agli utenti autorizzati e deve essere effettuato con username e password assegnati dall'Amministratore di Rete o formale responsabile.

La password non deve essere scritta su alcun supporto né cartaceo né magnetico né di altra natura.

La password non deve essere divulgata ad altre persone compresi i dipendenti. L'account è strettamente personale e non deve essere ceduto ad altri nemmeno temporaneamente, ad esempio consentendo l'accesso ad altre persone con il proprio account, oppure lasciando incustodito il sistema su cui si è effettuato il login.

Le password hanno una durata limitata nel tempo. Oltre tale limite il sistema richiede all'utente il cambio d password. Inoltre le ultime cinque password inserite, non possono essere riutilizzate.

La password non può essere costituita da una parola presente nei vocabolari italiano ed inglese. La stessa password non è valida nemmeno se preceduta o seguita da una o due cifre.

E' inoltre buona usanza creare password che rendano difficile un attacco dall'esterno al SIA. In particolare, si consiglia la creazione di password di lunghezza rilevante e che possano essere ricordate con facilità (parole senza vocali, acronimi di frasi, simboli di punteggiatura, ecc).

Ogni utente si impegna a non fornire a terzi indicazioni o istruzioni che possano essere idonee a consentire l'accesso ai SIA.

Un utente non può in alcun modo tentare di accedere fraudolentemente a dati/programmi a cui non è esplicitamente abilitato, né tentare di accedere come utente privilegiato. Ogni tentativo di accedere fraudolentemente è considerato violazione grave delle Condizioni Generali di Utilizzo, e dà diritto al Dirigente di perseguire con azioni disciplinari e/o legali l'utente che ha commesso la violazione.

La connessione di PC o Notebook al SIA è consentita solo se la macchina è stata preventivamente registrata dall'Amministratore di Rete e configurata secondo gli standard in uso presso VI Circolo.

Eventuali richieste di interventi di terzi sul SIA, dovranno essere comunicate all'Amministratore di Rete, nella sua qualità di responsabile della sicurezza dei sistemi informativi, che provvederà alle valutazioni del caso, ed alla necessaria autorizzazione, tenendo annotati tali interventi.

8. Utilizzo del SIA

Ogni utente si impegna a non utilizzare hardware, software, dati, il proprio login per uso personale essendo, l'uso del SIA, consentito solo per le attività necessarie ai processi di business.

Il luogo di lavoro è costituito dai locali del VI Circolo.

Pertanto, ogni utente si impegna a non trasferire in nessun caso fuori da detti locali hardware, software e dati.

Non è consentito l'utilizzo del SIA per attività illegali, o che possano procurare danno all'Istituzione Scolastica, ai suoi collaboratori, fornitori, clienti.

Gli utenti che devono effettuare prestazioni lavorative presso terzi, dovranno essere autorizzati dal rispettivo Capo Reparto/Ufficio, che dovrà a sua volta darne comunicazione preventiva al Capo Reparto Servizi Generali e Assicurazione Qualità nella sua qualità di coordinatore delle attività relative al SIA.

E' compito dell'utente collaborare con l'Amministratore del Sistema e con i suoi delegati per consentire il miglioramento del SIA.

9. Riservatezza dei dati, dei programmi e della conoscenza aziendale

All'Amministratore di Rete è fatto obbligo di fornire le linee guida, gli strumenti e le procedure per mantenere l'integrità:

- dei dispositivi costituenti la rete aziendale.
- delle basi di dati costituenti il SIA.
- degli account assegnati agli utenti del SIA.

Tali linee guida costituiscono le politiche di amministrazione del SIA.

Esse sono definite dall'Amministratore del Sistema e devono essere scrupolosamente osservate dall'utenza.

L'utente è responsabile della salvaguardia delle informazioni usate e/o memorizzate sul SIA con il proprio account.

I dati presenti sul SIA sono considerati riservati, e non devono in alcun modo essere divulgati a terzi senza consenso esplicito del proprietario. Ogni divulgazione non autorizzata è considerata violazione grave delle Condizioni Generali di Utilizzo e dà il diritto al Dirigente di perseguire con azioni disciplinari e/o legali l'utente cha ha commesso la violazione.

Ogni utente si impegna a mantenere riservati i dati concernenti persone fisiche e giuridiche che interagiscono con il SIA, nonché le informazioni relative alle attività di terzi di cui venga a conoscenza in relazione all'effettuazione del proprio lavoro sul SIA.

I dati di terze parti possono essere memorizzati nel SIA solo con l'esplicito assenso dell'interessato.

Notebook e PC non devono contenere dati riservati se non per il tempo strettamente necessario al loro trattamento, ed in ogni caso devono essere protetti come minimo applicando le autorizzazioni alle directory che li contengono e abilitando l'accesso con username e password.

I supporti utilizzati per il trasferimento dei dati devono essere cancellati prima e dopo il loro utilizzo, al fine di evitare fughe indesiderate di dati.

Ogni utente si impegna a mantenere segreto il contenuto dei programmi sviluppati da Argo e a proteggere i diritti dello stesso.

Ogni utente si impegna a mantenere segreti i concetti, le idee, il know-how, le tecniche e le procedure relativi all'elaborazione dei dati o programmi sviluppati presso il VI Circolo.

Detti concetti, idee, know-how, tecniche e procedure costituiscono patrimonio esclusivo del VI Circolo di Caltanissetta.

10. Uso della posta elettronica e di Internet

L'uso della posta elettronica e di internet sono consentiti solo per le attività necessarie ai processi di insegnamento e alle procedure amministrative.

La posta elettronica non deve essere utilizzata per comunicazioni riservate o per la trasmissione di dati riservati.

Tale mezzo di comunicazione non è sicuro (non esistono garanzie sull'arrivo a destinazione del messaggio, sulla sua integrità e sulla certezza dell'arrivo ai soli destinatari) e va integrato con meccanismi di crittografia a chiave pubblica, previo accordo con il destinatario e con l'autorizzazione dell'Amministratore di Sistema.

La responsabilità di un messaggio inviato via posta elettronica, ricade per intero sul suo creatore.

Non è consentito l'uso della posta elettronica per diffondere "catene di S. Antonio", virus, programmi pirata o in violazione della Legge Italiana.

Ogni file ricevuto via posta elettronica o da Internet deve essere preventivamente verificato con un antivirus, e nel dubbio deve essere contattato dell'Amministratore di Sistema.

Ogni file inviato per posta elettronica deve essere preventivamente compresso per minimizzare l'utilizzo della banda.

Internet è un mezzo di comunicazione potenzialmente dannoso: chi cagiona danno anche involontariamente, se ne assume la piena responsabilità.

Su Internet non sono consentite attività che esulino dal proprio compito in azienda. In particolare non è permessa la partecipazione a canali di chat, lo scaricamento di file mp3, l'uso indiscriminato della posta elettronica, ecc.

Queste attività, oltre a non appartenere all'ambito lavorativo, degradano anche in misura determinante le prestazioni del SIA (si veda il paragrafo 11).

Ogni utente si impegna a non intercettare comunicazioni informatiche di terzi.

11. Utilizzo del software

In generale vale il principio per cui gli utenti devono rispettare i copyright, le licenze ed altre informazioni on-line relative ai prodotti software trattati.

E' consentito il solo uso di software regolarmente registrato dal VI Circolo oppure freeware o di pubblico dominio (non sono ammesse, quindi, copie non autorizzate di programmi). Si veda anche il primo punto del paragrafo 7.

Non è consentita la copia di software in violazione del copyright, eccetto per i casi consentiti dalla legge (backup).

E' vietata l'installazione di nuovo software o la modifica di quello già installato, senza espressa autorizzazione del responsabile della sicurezza dei sistemi informativi.

Non è consentito l'utilizzo di programmi copiatori o altri dispositivi di copia per scopi diversi da quelli del salvataggio dei dati e di gestione ordinaria degli stessi.

Si ricordi che la violazione delle leggi in vigore in materia di software, comporta due grandi categorie di reati:

Quella relativa alla duplicazione di programmi per fini di lucro (v. art. 171 bis e seguenti leggi n. 633/41)

Quella relativa a danni provocati ad impianti di pubblica utilità o a sistemi informatici e telematici (v. legge n. 547/93), con l'aggravante in caso di reato commesso da incaricato di pubblico servizio (tali sono considerati i lavoratori della aziende di pubblici servizi locali).

Il mancato rispetto della regolamentazione riportata può dare luogo all'applicazione anche delle sanzioni disciplinari previste dal vigente C.C.N.L.

Si riporta per conoscenza un estratto delle citate leggi.

L'art. 171 della L. n. 633/41 sul diritto d'autore dispone: "E' punito con la multa da £. 100.000 a £. 4.000.000 chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma:

riproduce (...), diffonde (...), un'opera altrui;

...omissis...

riproduce un numero di esemplari (...) maggiore di quello che aveva diritto di produrre

...omissis...

Rientra in questa fattispecie il caso di colui che copia il software per uso personale.

L'art. 171 bis della citata legge così dispone: "Chiunque abusivamente duplica a fini di lucro, programmi per elaboratore o, ai medesimi fini sapendo o avendo motivo di sapere che si tratta di copie non autorizzate, importa, distribuisce, vende, detiene a scopo commerciale, o concede in locazione i medesimi programmi, è soggetto alla pena della reclusione da tre mesi a tre anni e della multa da £. 500.000 a £. 6.000.000. Si applica la stessa pena se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale dei dispositivi applicati a protezione di un programma per elaboratore. La pena non è inferiore nel minimo a sei mesi di reclusione e la multa di £. 1.000.000 se il fatto è di rilevante gravità ovvero se il programma oggetto dell'abusiva duplicazione, importazione, distribuzione, vendita, detenzione a scopo commerciale o locazione sia stato precedentemente distribuito, venduto o concesso in locazione su supporti contrassegnati dalla SIAE...omissis..."

La Legge n. 547/93 punisce, invece, i seguenti crimini informatici: alterazione, modificazione e cancellazione di un programma informatico; impedimento e turbamento del funzionamento di un sistema informatico; falsificazione di un documento informatico; accesso abusivo ad un sistema informatico; detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici; diffusione di programmi diretti a danneggiare o interrompere un sistema informatico; intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche; installazione di apparecchiature atte ad intercettare, impedire e interrompere comunicazioni informatiche o telematiche; danneggiamento di sistemi informatici e telematici.

12. Integrità del SIA

L'utente non deve deliberatamente svolgere attività atte a degradare le prestazioni del SIA, intendendo con questo l'utilizzo di software che compia elaborazioni intensive che possano bloccare il sistema, oppure l'utilizzo sconsiderato di banda internet o intranet, oppure la memorizzazione di dati sui supporti magnetici del SIA che occupi spazio oltre il necessario.

L'utente non deve divulgare a terzi le informazioni riguardo alla configurazione del SIA, i numeri telefonici di accesso, l'architettura di rete o le procedure di gestione ed utilizzo senza l'autorizzazione scritta.

L'utente non è autorizzato ad utilizzare software che possano compromettere l'integrità del SIA, come ad esempio network sniffers, password cracker, virus, security scanner o altri.

E' responsabilità del solo Amministratore di Sistema utilizzare software come network sniffers, password cracker, security scanner al solo scopo di migliorare la sicurezza del SIA.

Il SIA contiene diversi log che registrano le attività degli utenti, con il fine di fornire informazioni sulla gestione del SIA, di migliorarne l'efficacia e l'efficienza e di evidenziare eventuali violazioni alle Condizioni Generali di Utilizzo. L'accesso è riservato all'Amministratore di Sistema.

Ogni utente si impegna a non danneggiare in alcun modo dati, programmi, documenti informatici e sistemi informatici aziendali. In particolare si impegna a non alterare, modificare o cancellare in tutto e in parte dati, programmi informatici, documenti informatici o sistemi informatici aziendali, o a impedire o turbare il

funzionamento di sistemi informatici o telematici aziendali. L'utente si impegna inoltre a non modificare, senza autorizzazione dell'Amministratore di Sistema , l'hardware del computer a propria disposizione. Si veda anche l'ultimo punto del paragrafo 10.

Ogni utente si impegna a non diffondere programmi virus a programmi comunque idonei ad arrecare danno ai sistemi informatici aziendali.

13. Notifica delle violazioni delle Condizioni Generali

Gli utenti sono tenuti ad informare tempestivamente l'Amministratore di Sistema relativamente a problemi riguardanti l'integrità, la riservatezza e la disponibilità dei dati.

L'amministratore di Sistema provvede quindi ad informare il responsabile di competenza, in funzione della gravità dell'accaduto.

Verranno effettuate periodiche verifiche a cura dell'Amministratore di Sistema , anche senza preavviso, per controllare la regolare applicazione delle disposizioni.