REGOLAMENTO SERVIZIO INFORMATICO

I.S.S.I.T.P.

“GIOVAN BATTISTA FERRIGNO”

rev	Descrizione	Data	Approvazione
00	Prima emissione	30.11.2018	Direzione

INDICE

PREMESSA

La presenza sempre più rilevante dell'informatica a vari livelli all'interno della struttura si e l'introduzione di una rete di personal computer, tutti dotati di una propria unità elaborativa, introduce l'obbligo di stabilire alcune regole fondamentali di approccio alla nuova filosofia client /server, e di utilizzo del nuovo sistema.

Al fine di limitare i danni e gli inconvenienti che una gestione non corretta del sistema può causare, vengono elencate di seguito le principali e minime attività e regole da seguire.

Attualmente, tutte le postazioni di lavoro trattano, in maniere più o meno preponderante, dati personali e solo alcuni di essi dati sensibili/giudiziari.

Sulla base di tali presupposti ogni settore, di concerto con la Direzione definirà le misure idonee di sicurezza per il loro trattamento , secondo le disposizioni dettate dalla normativa vigente sulla tutela dei dati personali (Regolamento Europeo 2016/679).

Il presente regolamento ha, pertanto, come finalità quello di garantire un corretto utilizzo del sistema informativo, assicurando, nel contempo, il rispetto delle norme sul trattamento dei dati e la sicurezza degli stessi.

Art. 1 - DEFINIZIONI

Ai fini del presente regolamento s'intende per:

- **Amministratore di Sistema (ADS):** il soggetto al quale è conferito il compito di sovrintendere alle risorse del sistema operativo e di consentirne l'utilizzazione. Tale soggetto utilizza un codice identificativo personale di accesso al sistema gestito secondo le specifiche standard di advanced security, ed è inoltre abilitato ai comandi low-level di sistema operativo

- **Assistenti di supporto:** sono operatori specializzati in procedure informatiche e, quei dipendenti individuati per iscritto dal Titolare, che svolgono funzioni elementari di supporto informatico all'interno dei servizi del Settore di appartenenza con compiti di ordinaria manutenzione. Essi, provvedono alle segnalazioni all'ADS di problemi hardware e software dei personal computer assegnati, e si rapportano con l'ADS per periodici aggiornamenti organizzativo-tecnici del lavoro su reti.

- **Dato Personale**: Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»), direttamente o indirettamente, con un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale

- **Dato sensibile/particolare**: E' il dato personale idoneo a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione ai partiti, sindacati associazioni od organizzazioni a carattere religioso,

filosofico, politico o sindacale, nonché i dati personali idonei a rilevare lo stato di salute e la vita sessuale dell'interessato

- **Dato Giudiziario**: dati personali idonei a rivelare i provvedimenti giudiziari penali ed amministrativi in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato

- **Data Protection Officer**: quale Responsabile della protezione dei dati personali , nominato dal Titolare e con l'obbligo di informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti e di sorvegliare l'osservanza del RGPD, fungere da punto di contatto con il Garante.

Art. 2 - UTILIZZO DELLA RETE

Le risorse hardware (personal computer, stampanti , server di rete) sono collegate fra di loro secondo un'architettura che consente di coniugare flessibilità e razionalità di utilizzo.

La condivisione di risorse permette, a chiunque ne abbia titolo e secondo specifiche autorizzazioni, l'utilizzo delle risorse disponibili.

Nell'ambito dei supporti di memorizzazione di massa del server l'Amministratore di Sistema mette a disposizione delle cartelle condivise, che sono poi rese disponibili sotto forma di unità logiche, per tutte le postazioni autorizzate ad accedervi. Il Titolare provvede a comunicare all'ADS i livelli di accesso e relative possibilità di utilizzo per ogni singolo utente, nonché eventuali necessità che dovessero presentarsi.

Art. 3 - IMPOSTAZIONI DELLA RETE

Ogni singolo Personal Computer accede alla rete tramite apposito codice di identificazione associato ad una parola chiave riservata, conosciuta solo dall'incaricato interessato, ed è univocamente definito da un indirizzo IP.

Ogni incaricato può disporre di una o più credenziali per l'autenticazione.

L'ADS conserva apposita tabella contenente la relazione fra ogni singola postazione, il suo ID di rete ed il relativo indirizzo IP.

La password può essere sostituita da un dispositivo di autenticazione in possesso e uso esclusivo dell' incaricato, oppure in una caratteristica biometria (dell'incaricato), eventualmente associata a un codice identificativo o a una parola chiave.

Proprio per consentire le funzionalità dell'architettura (condivisioni, utilizzo di diverse risorse da ogni singola postazione, ecc.) è vietata qualsiasi modifica alle impostazioni, connessioni o condivisioni create dall'ADS.

Art. 4 - PASSWORD

Ogni personal computer, deve, essere dotato di password, composta da almeno otto caratteri alfanumerici.

La password, inoltre, non deve contenere riferimenti agevolmente riconducibili all'incaricato (es. data di nascita oppure uguale al nome utente), ma deve, invece, essere modificata almeno ogni tre mesi sia se si trattino dati personali, dati sensibili e/o dati giudiziari

La medesima password non può essere assegnata ad altri incaricati, neppure in tempi diversi.

L'Istituto per garantire una maggiore sicurezza agli accessi ai sistemi informatici ha stabilito l'utilizzo di almeno tre password:

1. password di accesso al sistema operativo risorsa ,

2. login e password di accesso alla rete (tramite verifica del dominio NT),

3. login e password di accesso al software applicativo di pertinenza.

Le stampanti sono in rete .

Ogni tre mesi l'ADS provvederà a sostituire le password di rete e di applicazione di ogni singolo utente, disattivando definitivamente e senza possibilità di riutilizzo quelle fino a quel momento in uso.

I codici identificativi personali dovranno essere gestiti in modo che ne sia prevista la disattivazione in caso di perdita della qualità che consentiva l'accesso all'elaboratore. Se verrà meno la qualità che aveva consentito l'attribuzione del codice identificativo personale (per esempio risoluzione del rapporto di lavoro) lo stesso codice non potrà essere attribuito a un nuovo dipendente.

I codici identificativi individuali sono strettamente personali e non devono essere comunicati ad alcuno. Sono consegnati individualmente ad ogni dipendente/collaboratore che ne è, pertanto, pienamente responsabile. Qualora l'ADS, tramite il normale monitoraggio delle connessioni verificasse che le stesse sono state utilizzate da dipendente/collaboratore diverso rispetto a quello assegnatario, provvederà immediatamente e per iscritto a darne comunicazione alla Direzione.

Tale riservatezza è necessaria in quanto il personal computer collegato in rete costituisce un possibile punto di accesso anche per gli altri personal e quindi potrebbe permettere ad altri dipendenti non autorizzati (o a terzi esterni all'Istituto) di accedere anche a dati sensibili in evidente violazione delle norme sulla sicurezza dei dati stessi.

E' fatto assoluto divieto ai dipendenti addetti alla gestione di ogni personal computer

dell’utilizzo dello stesso ad altro personale od estranei all’ufficio che non sia dipendente di ditte che abbiano la manutenzione del software o dell’Hardware, dell’apparecchiatura informatica ad essi assegnata attraverso apposite lettere d’incarico.

Al termine dell'orario di lavoro, intendendo per termine anche la sospensione per la pausa del pranzo, o in caso di assenza di durata tale da non consentire la sicurezza dei dati della singola postazione, il personal computer deve essere lasciato in modalità non accessibile da terzi (Lock su sistemi NT, con software apposito o quantomeno con screen saver protetto da password).

Art. 5 - ABILITAZIONE CODICI IDENTIFICATIVI

Per l'attribuzione dei privilegi di accesso connessi al codice individuale identificativo che consente l'utilizzo di software applicativo specifico, i Funzionari responsabili di Settore faranno richiesta di accesso e utilizzo, in forma scritta, all’ADS, indicando esplicitamente i diversi gradi di capacità (gestione, interrogazione, ecc.) per il Personale incaricato dei vari servizi, elencando inoltre i "menù" (se presenti) del programma ritenuti strettamente necessari alla funzionalità dell'operatore, in relazione alle funzioni a ciascuno assegnati.

Nel caso fosse evidenziata la necessità di un collaboratore/dipendente di accedere, in sola consultazione, ai dati di competenza di altro Settore, la richiesta di abilitazione a tali "menù" dovrà essere approvata dal Titolare.

L’ADS non è tenuto ad abilitare accessi, anche in sola consultazione, in mancanza della richiesta ed approvazione del Titolare.

Art. 6 - PROGRAMMI ANTI-INTRUSIONE (ANTIVIRUS-ANTIMALWARE)

La presenza dei cosiddetti virus è un problema da affrontare con le dovute serietà e cautele e soprattutto con la consapevolezza che il mancato rispetto delle regole può essere dannoso sia al proprio personal, e quindi al proprio lavoro, che a quello degli altri, se non addirittura a quello dell'intera struttura nel caso si " infetti" il server centrale.

Per questo motivo nel presente articolo si descrivono le precauzioni che ciascun utente è tenuto ad osservare.

Su ogni postazione di lavoro viene installato un programma antivirus, che opererà normalmente anche in background per uno scanning continuo dei dati utilizzati. In caso di mancanza o malfunzionamento di questo software (per reinstallazione del sistema operativo o altre cause), l’operatore è tenuto a segnalare l’evento all’ADS con la massima urgenza.

Dei programmi "antivirus" già installati vengono fornite, regolarmente e con cadenza quanto meno settimanale, versioni aggiornate, per consentire la massima sicurezza possibile rispetto ai "virus" fino a quel momento noti.

In quest'ultimo caso gli assistenti di supporto sono tenuti ad effettuare tempestivamente le procedure, secondo le modalità indicate dall'ADS, dando conferma scritta allo stesso della regolare esecuzione, segnalando nel dettaglio i virus eventualmente riscontrati.

Art 6.1. FATTORI DI INCREMENTO DEL RISCHIO E COMPORTAMENTI DA EVITARE

E' assolutamente vietato

- utilizzo di pen drive ;
- l'uso di software gratuito (o shareware) prelevato da siti Internet o in allegato a riviste o libri non autorizzato dall'amministratore di rete nonché dal DPO;
- il collegamento in rete, nel quale il client avvia solo applicazioni residenti nel proprio disco rigido o in cloud nel caso del gestionale;
- il collegamento in rete, nel quale il client avvia anche applicazioni residenti sul disco rigido del server e in terminale server;
- ricezione di applicazioni dall'esterno.
- l'utilizzo dello stesso computer da parte di più persone se non autorizzati;
- collegamento in Internet con download di file eseguibili o documenti di testo da siti web o da siti FTP non sicuri o autorizzati;
- collegamento in Internet e attivazione degli applets di Java o altri contenuti attivi se non autorizzati;
- file attached di posta elettronica di dubbia provenienza.Nel caso di presenza di virus, anche se rimosso automaticamente, il personal computer "infetto" non dovrà essere usato per alcun motivo fino alla bonifica. Il software antivirus:

1. non deve essere mai disabilitato;

2. deve risultare attivo per ogni "file";

3. deve essere eseguito su tutto l'Hard Disk,

4. deve essere eseguito ogni volta che viene utilizzato una pendrive o un CD Rom.

Art. 6.2 PREVENIRE CONTAGIO DA VIRUS

Si consiglia:

1. **l'utilizzo di programmi provenienti solo da fonti fidate,** copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato.

2. **Non si deve utilizzare il proprio "disco sistema" su di un altro** computer se non in condizione di "protezione in scrittura".

3. **Assicurarsi che il software antivirus sia aggiornato,** La tempestività nell'azione di bonifica è essenziale per limitare i danni che un virus può causare;

4. **Non diffondere messaggi di provenienza dubbia quali email senza oggetto, o che avvisano di un virus pericolosissimo**

5. **Non partecipare a catene di Sant'Antonio e simili. Analogamente, tutti i messaggi che vi invitano a "diffondere la notizia quanto più possibile" sono hoax (cioè bufale). Per agevolare il lavoro degli utenti l'ADS potrà predisporre delle procedure automatizzate** di scansione da effettuarsi in momenti di inattività degli uffici (all'orario di chiusura).

L'ADS dovrà segnalare, in forma scritta, al Titolare e al DPO, ogni eventuale anomalia e difformità riscontrata, rispetto a quanto indicato, al fine di adottare i necessari provvedimenti per il mantenimento della sicurezza del Sistema.

Art. 7 INTERNET , FIREWALL E MAIL

Allo stato attuale, su reti LAN chiuse, i rischi maggiori per la sicurezza derivano dall'utilizzo di collegamenti ad Internet operati da postazioni connesse alla rete locale. Per questo motivo queste postazioni devono rispettare protocolli di sicurezza più elevati rispetto a quelli degli altri Personal Computer.

E' fatto assoluto divieto di effettuare connessioni diverse da quelle impostate dall'ADS in "Accesso Remoto", anche per motivi di teleassistenza, senza la previa verifica dello stesso.

L'ADS predispone le necessarie impostazioni di sistema per l'accesso alla rete Internet e relativi servizi di E-mail. Per i motivi di sicurezza sopra citati, e per impedire l'accesso a persone non autorizzate, gli utenti non dovranno nel modo più assoluto avvalersi delle funzioni di memorizzazione delle password contenute nei programmi di navigazione e client di E-mail.

A sicurezza di ciò è stato installato sistema di firewall.

Durante la navigazione l'addetto dovrà limitarsi ad accedere ai siti connessi con le attività dell'Istituto, evitando con particolare cura tutti quelli che non presentino le massime garanzie in termini di sicurezza. Per ulteriore precauzione le funzioni di verifica dei "cookies", delle applet Java e degli script ActiveX dovranno essere comunque attivate, e l'operatività degli stessi consentita solo se sussistono le condizioni minime di sicurezza. A sicurezza di ciò è installato apposito sistema proxy

Tutto il materiale proveniente da Internet, nonché gli attachment di E-mail, dovranno essere sottoposti a verifica con software antivirus avente le firme aggiornate, essendo estremamente elevato il rischio di contrarre virus anche di recente produzione.

Art. 8 - DOTAZIONE SOFTWARE

Ogni personal computer e, più in generale, ogni attrezzatura informatica, ha in dotazione software di utilità forniti su rilascio di regolare licenza.

La legge che disciplina i diritti d'autore (L. 22 aprile 1941 n. 633), aggiornata dal Dl. 29.12.1992, n.518, che ha recepito la direttiva CEE n. 250 del 14.05.1991 relativa alla tutela giuridica del software, prevede che la sua duplicazione, salvo apposito contratto, oltre al numero di licenze regolarmente acquistate, sia reato perseguibile anche penalmente.

Pertanto, ogni software installato sulle attrezzature in dotazione agli Uffici dovrà essere corredato da regolare licenza.

Tutte le licenze, anche quelle che verranno nel tempo acquisite, devono essere consegnate al SI che ne curerà la registrazione e le conservazioni. Installare le Patch di aggiornamento dei sistemi operativi e dei programmi utilizzati per il trattamento dati personali, con cadenza annuale che diviene semestrale in caso di trattamenti di dai sensibili o giudiziari

Al fine di tenere aggiornato il patrimonio informatico in dotazione, nonché per rendere più snella l'attività di manutenzione, l'ADS predisporrà una scheda, sottoscritta anche dall'utente assegnatario, per ogni singola attrezzatura, indicante le caratteristiche della stessa (marca, modello, numero di matricola, numero di inventario, ecc.) e il software installato.

Ogni software non indicato nella suddetta scheda è da considerarsi privo di regolare licenza e pertanto di ritenere non autorizzato e assimilabile a "software pirata".

E' fatto assoluto divieto ad ogni addetto di effettuare l'installazione di qualunque tipo di software, anche se dotato di regolare licenza, senza previo assenso dell'ADS, che verificherà preventivamente le caratteristiche del prodotto e le eventuali ripercussioni che una sua installazione potrebbe avere sul buon funzionamento della singola postazione o dell'intera LAN.

I singoli assegnatari dovranno rispondere di ogni eventuale difformità riscontrata. L'ADS è tenuto a segnalate, in forma scritta per i provvedimenti anche disciplinari del caso ogni eventuale installazione non registrata.

I supporti informatici di vario genere, spesso allegati gratuitamente a riviste e periodici, non sempre sono di buona qualità. Inoltre alcuni prodotti di tipo "shareware" (cioè privi di licenza) in genere risultano non soggetti a copyright solo per soggetti privati. Perciò, se ne vieta categoricamente l'impiego a meno di una specifica autorizzazione da parte dell'ADS

E' vietata l'installazione di programmi di intrattenimento, giochi e quant'altro non attinente all'attività lavorativa o a piattaforme online e siti tipo: facebook, twitter, youtube, etc... , tranne ai soggetti autorizzati e solo per motivi lavorativi.

L'attivazione di screen-saver, in quanto in grado di determinare un notevole degrado di prestazioni in sistemi operativi di tipo "Windows", dovrà essere effettuata con la supervisione dell'ADS, che curerà altresì che, in mancanza di altro software all'uopo dedicato, siano attivate le funzioni di protezione dello screen-saver medesimo.

Per quanto sopra esposto, l'ADS eventualmente supportato dal DPO è tenuto ad effettuare periodici controlli su ogni postazione di lavoro e a segnalare in forma scritta eventuali inadempienze.

Art 9 - ACQUISTI

Al fine di garantire la compatibilità delle singole componenti con l'intero sistema informatico e di mantenere una standardizzazione dei prodotti, anche per un miglior utilizzo delle risorse disponibili, per ogni acquisto di materiale informatico, sia hardware che software, dovrà essere acquisito preventivamente il parere di conformità del DPO e dell'ADS.

Art. 10 - SICUREZZA LOGICA

Oltre che con le modalità precisate negli articoli precedenti (codici identificativi individuali, autorizzazioni specifiche per l'accesso selezionato ai dati, programmi antivirus, periodici controlli, ecc.) l'integrità e la sicurezza dei dati devono essere garantite da rischi di distruzione e perdite accidentali (comandi applicativi c/o operativi errati, presenza nonostante tutto, di virus, malfunzionamenti dell'hardware, ecc.).

E' pertanto obbligatorio procedere giornalmente, a cura dell'ADS, a effettuare le procedure di salvataggio giornaliere, adottando un sistema di rotazione dei supporti su dischi rigidi e garantendone la conservazione periodica in luoghi quali hardisk esterni o in cloud e con protocolli di criptazione che ne aumentino la sicurezza in caso di tentato accesso non autorizzato

Art. 11 SICUREZZA FISICA

È preciso dovere di ciascuno, secondo le funzioni e le relative responsabilità, fare in modo che vengano utilizzati scrupolosamente tutti gli accorgimenti atti ad evitare indebite intrusioni negli locali scolastici (controllo degli accessi alla struttura tramite portierato, e sistema di videosorveglianza, chiusura a chiave dei contenitori e dei luoghi ove vengono conservati dati e attrezzature.)

Altresì la zona di attesa degli utenti deve essere distanziata dagli archivi elettronici e cartacei ed è, inoltre, sempre auspicabile che sia presente un controllo da parte degli addetti.

Art. 12 TRATTAMENTO DEI DATI SENZA L'AUSILIO DEGLI STRUMENTI ELETTRONICI

Tutti i documenti cartacei devono essere gestiti in modo da ridurre al minimo i tempi di permanenza al di fuori degli archivi o degli armadi o contenitori in dotazione alle unità operative. Massima attenzione dovrà essere posta per i documenti che si trovano in locali accessibili al pubblico. L'accesso agli archivi è consentito al personale a ciò espressamente autorizzato in via permanente od occasionale. Gli archivi sono tenuti costantemente chiusi, compatibilmente con le esigenze di lavoro. Qualsiasi persona ammessa, dopo l'orario di chiusura, deve essere identificata e registrata.

E' considerata negligenza e trattata nei modi previsti dalla normativa vigente, anche la mancata segnalazione di eventuali anomalie casualmente riscontrate da parte di chiunque ne venga a conoscenza. Le copie dei documenti sono trattate, con riferimento alla tutela dei dati personali in esse contenuti, con la medesima diligenza riservata agli originali.

Gli addetti ai servizi dove possono essere trattati dati sensibili o giudiziari dovranno porre la massima attenzione al rispetto delle disposizioni precedenti. Essi dovranno inoltre limitare al minimo indispensabile la giacenza della documentazione al di fuori degli armadi o contenitori muniti di serratura; ognuno degli incaricati dovrà controllare con particolare rigore sia l'accesso ai propri archivi che egli eventuali accessi negli uffici compiuti al di fuori degli usuali orari di chiusura mediante registrazione in apposito elenco/registro ove predisposto.

Si è disposto che non siano lasciati incustoditi sulle scrivanie, o su altri ripiani, atti, documenti e fascicoli delle pratiche. I fascicoli devono essere classificati in maniera da ridurre al minimo l'identificazione da parte di terzi e non devono rivelare il loro contenuto e vanno conservati nell'apposito faldone della stanza archivio e prelevati esclusivamente per il tempo necessario al trattamento per esservi poi riposti. Si è data espressa disposizione agli incaricati che tutte le comunicazioni a mezzo posta, o mezzo fax, dovranno essere tempestivamente smistate e consegnate ai destinatari. Quando è dato un ordine di stampa, il documento dovrà essere prontamente prelevato dalla stampante e consegnato all'interessato.

Si è data istruzione che tutto il materiale cartaceo asportato e destinato allo smaltimento dei rifiuti sia preventivamente distrutto (anche con l'ausilio di appositi strumenti distruggi carta), cancellato e tagliato e poi riposto negli appositi sacchi di plastica e che detti sacchi siano richiusi in modo che atti e documenti negli stessi contenuti non possano accidentalmente fuoriuscire, e che detto materiale sia giornalmente asportato. Alle ditte che per qualsivoglia motivo provvedano ad effettuare prestazioni che comportano accessi di estranei alle strutture dello studio, viene dato incarico scritto con richiesta di specificazione dei nominativi delle persone che accedono ed espresso invito a limitarsi alle sole attività pertinenti alla prestazione per cui accedono.