Regolamento interno per l'utilizzo di strumenti e tecnologie informatiche dell'A.S.P. ITIS

(approvato con del. n. 48/12 dd. 11.12.2012)

Indice

Art. 1 Campo di applicazione

Il presente regolamento si applica a tutti i dipendenti dell'A.S.P. ITIS, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'Azienda a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratori a progetto, in stage, ecc.) ed a chiunque altro dovesse utilizzare le risorse informatiche dell'Azienda.

Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni utilizzatore a cui vengono concesse specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata quale "incaricato del trattamento".

Art. 2 Utilizzo del Personal Computer

Il Personal Computer affidato all'utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa o aziendale è vietato, in particolare: qualora causi disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza, ovvero ostacoli l'attività dell'Amministrazione o sia destinato al perseguimento di interessi privati in contrasto con quelli aziendali. Il Personal Computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento o l'utilizzo indebito da parte di altre persone.

Il Personal Computer dato in affidamento all'utente permette l'accesso alla rete dell'Azienda solo attraverso specifiche credenziali di autenticazione come meglio descritto al successivo articolo 3 del presente Regolamento.

Il personale incaricato dal Servizio Tecnico aziendale è autorizzato a compiere interventi nel sistema informatico aziendale, diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, ecc.). Detti interventi, in considerazione dei divieti di cui ai successivi articoli 7, comma 3, ed 8, comma 1, potranno anche comportare l'accesso in qualunque momento ai dati trattati da ciascuno nel rispetto della normativa vigente in materia di tutela della riservatezza dei dati personali. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Azienda, si applica anche in caso di assenza prolungata od impedimento dell'utente.

Il personale incaricato dal Servizio Tecnico aziendale ha la facoltà di collegarsi in remoto nelle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, ecc.. L'intervento viene effettuato su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria

tempestività ed efficacia dell'intervento, verrà data comunicazione all'utente della necessità dell'intervento stesso.

Tecnici incaricati esterni (es. fornitori di sofware in uso in azienda) sono autorizzati ad effettuare interventi in remoto al server aziendale, esclusivamente se autorizzati e sotto la supervisione del personale incaricato dal Servizio Tecnico; se l'intervento viene effettuato sui client, l'autorizzazione e la supervisione sono a carico del singolo utente.

Non è consentito, salvo casi eccezionali appositamente autorizzati, l'uso di programmi diversi da quelli ufficialmente installati dal personale incaricato dal Servizio Tecnico per conto dell'Azienda, né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della suddetta disposizione espone la stessa Azienda a gravi responsabilità civili; si evidenzia inoltre che la normativa vigente a tutela dei diritti d'autore sul software richiedono la presenza nel sistema di software con regolare licenza o comunque libero e quindi non protetto dal diritto d'autore e le violazioni a tale normativa vengono sanzionatew enche penalmente.

Salvo preventiva espressa autorizzazione del personale incaricato dal Servizio Tecnico aziendale, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc.).

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna e nel caso in cui siano rilevati virus, deve avvertire immediatamente il personale incaricato dal Servizio Tecnico ed adottare quanto previsto dal successivo art. 9 del presente Regolamento relativo alle procedure di protezione antivirus.

Il Personal Computer e gli altri supporti utilizzati individualmente (es. stampante, scanner ecc.) devono essere spenti prima di lasciare gli uffici per fine giornata di lavoro o in caso di assenze prolungate dall'ufficio o in caso di inutilizzo. Viene infatti posto a capo del dipendente l'obbligo di impedire ad altri indebiti utilizzi della propria apparecchiatura informatica, non rilevando, al fine del difetto di responsabilità, il fatto che altri in sua assenza abbia potuto usare la postazione lavorativa. In difetto, il comportamento del dipendente si configura come negligenza inescusabile e gravemente colposa.

Art. 3 Gestione ed assegnazione delle credenziali di autenticazione

Le credenziali di autenticazione per l'accesso alla Rete Aziendale vengono inizialmente assegnate dal personale incaricato dal Servizio Tecnico e successivamente resettate dal dipendente stesso secondo criteri prestabiliti.

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dal Servizio Tecnico, associato ad una parola chiave (password) riservata, creata dall'incaricato e che dovrà essere memorizzata, custodita con la massima diligenza e non divulgata. In casi eccezionali il personale incaricato dal Servizio Tecnico è autorizzato a resettare le password di accesso ai personale computers dei singoli incaricati.

La parola chiave deve essere formata da 8 o più caratteri appartenenti ad almeno tre delle seguenti quattro categorie: lettere maiuscole, lettere minuscole, numeri, caratteri speciali, anche in combinazione fra loro, e non deve contenere riferimenti agevolmente riconducibili all'incaricato.

La password di accesso di ciascun incaricato sarà automaticamente resettata ogni tre mesi. In base a tale procedura automatica l'incaricato, mediante avviso a video, dovrà inserire ogni tre mesi una password nuova, diversa dalla precedente.

L'utente potrà richiedere la modifica della parola chiave al personale incaricato dal Servizio Tecnico, per decorrenza del termine sopra previsto e/o in caso di perdita della riservatezza.

Soggetto autorizzato alla modifica delle credenziali di autenticazione, per l'effettuazione di eventuali controlli, è l'apposito personale incaricato dal Servizio Tecnico.

Art. 4 Utilizzo della Rete

Per l'accesso alla rete dell'Azienda ciascun utente deve essere in possesso delle specifiche credenziali di autenticazione.

È assolutamente proibito entrare nella rete e nei programmi con il codice d'identificazione utente di un altro operatore. Le parole chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

Le cartelle utenti presenti nel "server storage" sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. I documenti di lavoro dovranno essere tutti memorizzati nelle cartelle di rete personali o in quelle relative all'ufficio di appartenenza. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in questa cartella. Su queste unità vengono svolte regolari attività di controllo, amministrazione e back up da parte del personale incaricato dal Servizio Tecnico. Tutti i dischi o altre unità di memorizzazione locali (es. disco C del proprio personal

computer) non sono soggette a salvataggio da parte del personale incaricato dal Servizio Tecnico, per cui la responsabilità del salvataggio dei dati eventualmente ivi contenuti è a carico del singolo utente.

Il personale incaricato dal Servizio Tecnico può in qualunque momento procedere alla rimozione di ogni file o applicazione che ritenga essere dannosa o pericolosa per la sicurezza sia sui personal computer degli incaricati sia sulle unità di rete.

Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei files obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

Art. 5 Utilizzo e conservazione dei supporti rimovibili

L'utente è responsabile della custodia dei supporti rimovibili e dei dati aziendali in essi contenuti.

Art. 6 Utilizzo di PC portatili

L'utente è responsabile del PC portatile assegnatogli in uso e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nei luoghi di lavoro, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

Ai PC portatili si applicano le regole di utilizzo previste dal presente regolamento, con particolare attenzione alla rimozione di eventuali file elaborati prima della riconsegna.

E' vietato connettersi alla rete aziendale attraverso qualsiasi dispositivo personale (PC portatile, smart phone, ecc.) non preventivamente autorizzato dal Servizio Tecnico.

Art. 7 Uso della posta elettronica

La casella di posta elettronica assegnata all'utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

Le caselle di posta elettronica sono accessibili a tutti i dipendenti aziendali ed ai collaboratori autorizzati specificando, in caratteri minuscoli, un identificativo costituito dal "proprio nome" + "." + "proprio cognome"+ "@itis.it"(per es. Mario Rossi accederà con mario.rossi@itis.it)

È fatto divieto di utilizzare le caselle di posta elettronica per i motivi sottoriportati:

- l'invio di allegati contenenti filmati o brani musicali (es. mp3) non legati all'attività lavorativa;
- l'invio di messaggi per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list, non strettamente legati all'attività lavorativa;

- la partecipazione a catene telematiche: non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi;
- l'invio di messaggi di natura rilevante e analoga a quelli sopra riportati;
- altri utilizzi diversi da quelli strettamente legati all'attività lavorativa, di portata analoga ai precedenti.

La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

È obbligatorio porre la massima attenzione nell'aprire i file allegati alle e-mail (attachements) prima del loro utilizzo e a non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti.

Nel caso in cui un utente di posta si assenti per più giorni (p.es. per malattia), sarà consentito a persona autorizzata dall'utente o comunque, sentito l'utente, a persona individuata dall'Azienda, accedere alla casella di posta elettronica, al fine di garantire la continuità del servizio lavorativo nel rispetto del principio di necessità e di proporzionalità.

Il personale incaricato dal Servizio Tecnico, nell'impossibilità di procedere come sopra indicato e nella necessità di non pregiudicare la tempestività ed efficacia dell'intervento, potrà accedere alla casella di posta elettronica per le sole finalità indicate all'art. 2, comma 3.

Art. 8 Navigazione in Internet

Il personal computer assegnato al dipendente ed abilitato alla navigazione in Internet costituisce uno strumento utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa.

In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare Internet per:

- l'accesso a siti internet aventi contenuti e/o finalità vietati dalla legge;
- l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web, se non strettamente attinenti all'attività lavorativa (ad. es. filmati e musica) e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato il personale incaricato dal Servizio Tecnico);
- l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dalla Direzione Generale (o eventualmente dal Responsabile d'Ufficio e/o del Servizio Tecnico aziendale) e comunque nel rispetto delle normali procedure di acquisto;

- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- la partecipazione a Forum non professionali, l'utilizzo di chat line, di social network (es. Facebook), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames), se non espressamente autorizzati dal Responsabile d'Ufficio;

Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'Azienda rende peraltro nota l'adozione di uno specifico sistema di blocco o filtro automatico che impedirà determinate operazioni quali l'accesso a siti internet aventi contenuti o finalità vietati dalla legge.

Gli eventuali controlli, compiuti dal personale incaricato del Servizio Tecnico ai sensi del precedente art. 2 comma 3, potranno avvenire mediante un sistema di controllo dei contenuti o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre 1 mese, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'Azienda.

Art. 9 Protezione antivirus

Il sistema informatico dell'Azienda è protetto da software antivirus aggiornato ogni tre ore. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo.

Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto al personale incaricato dal Servizio Tecnico.

Ogni CD o USB di provenienza esterna all'Azienda, prima del suo utilizzo, sarà automaticamente verificato mediante il programma antivirus e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale incaricato dal Servizio Tecnico.

Art.10 Utilizzo dei telefoni, fax e fotocopiatrici aziendali

Il telefono eventualmente affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa.

L'effettuazione di telefonate personali è consentita solo nel caso di comprovata necessità ed urgenza.

Qualora venisse assegnato un cellulare aziendale al dipendente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al cellulare si applicano le medesime regole sopra previste per l'utilizzo del telefono aziendale: in particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere telefonate, SMS o MMS di natura personale o comunque non

pertinenti rispetto allo svolgimento dell'attività lavorativa e in conformità delle istruzioni al riguardo impartite dal Direttore generale. E' tuttavia prevista la facoltà di adesione da parte dell'assegnatario alla cd. modalità "Dual billing", se adottata dall'Azienda, che consente tramite anteposizione di apposito codice numerico l'addebito di tutto il traffico effettuato a titolo privato.

L'utilizzo del cellulare viene autorizzato con il verbale di concessione in uso e consegna al titolare, che dichiara la piena responsabilità e la correttezza d'uso.

È vietato l'utilizzo dei fax per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte del Responsabile di Servizio.

È vietato l'utilizzo delle fotocopiatrici per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di Servizio.

Tutti i numeri chiamati e ricevuti vengono registrati su supporti informatici.

Art. 11 Osservanza delle disposizioni in materia di Privacy

E' obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicato nella lettera di designazione ad incaricato del trattamento dei dati ai sensi del Disciplinare tecnico allegato al D.Lgs. n. 196/2003.

Art. 12 Accesso ai dati trattati dall'utente

E' facoltà dell' Azienda, tramite il personale incaricato dal Servizio Tecnico, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali ed ai documenti ivi contenuti, nonché ai tabulati del traffico telematico, per motivi di sicurezza del sistema informatico, per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, ecc.), per finalità di controllo e programmazione dei costi (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.). L'accesso in ogni caso non dovrà essere finalizzato al controllo dell'attività lavorativa.

Art. 13 Sistemi di controlli graduali

In caso di anomalie, il personale incaricato dal Servizio Tecnico effettuerà controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti del Servizio in cui è stata rilevata l'anomalia, si evidenzierà l'utilizzo irregolare degli strumenti informatici e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie.

In alcun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

Art. 14 Sanzioni

È fatto obbligo a tutti gli utenti individuati all'art. 1 c. 1 di osservare le disposizioni portate a conoscenza con il presente regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile con i provvedimenti disciplinari e/o risarcitori previsti dalla vigente normativa, nonché con tutte le azioni civili e penali consentite.

Art. 15 Entrata in vigore del regolamento e pubblicità

Con l'entrata in vigore del presente Regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi sostituite dalle presenti.

Copia del regolamento verrà consegnata a ciascun Responsabile di Servizio per renderlo noto ai rispettivi collaboratori, nonché affisso in modo permanente in luogo visibile a tutti e pubblicato sul sito internet dell'Azienda.