Regole Comportamentali per la Sicurezza Informatica

Via D.Cirillo, 33
70126 Bari (BA),
codice univoco: UFOU5L
codice fiscale: 93257010723
email: bavc010004@istruzione.it –
pec: bavc010004@pec.istruzione.it

Revisione 2018-09-30 GDPR R00

Il titolare del trattamento, Convitto Nazionale Statale D. Cirillo Via D.Cirillo, 33 - 70126 Bari (BA), - codice univoco: UFOU5L - codice fiscale: 93257010723 - email: bavc010004@istruzione.it – pec: bavc010004@pec.istruzione.it, successivamente denominato Istituto, decide di adottare il seguente regolamento di sicurezza informatica.

Premessa

L'utilizzo delle risorse informatiche, telematiche e del patrimonio informativo del nostro Istituto deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che il collaboratore è sempre tenuto ad adottare nell'ambito del rapporto di lavoro.

Tuttavia poiché anche nella normale attività lavorativa alcuni comportamenti potrebbero mettere a rischio la Sicurezza e l'immagine dell'Istituto, di seguito vengono richiamate semplici regole comportamentali finalizzate non tanto a censurare comportamenti consapevolmente scorretti già di per se proibiti, ma soprattutto per evitare condotte che inconsapevolmente possano causare rischi alla Sicurezza Informatica dell'Istituto.

L'Istituto predispone momenti informativi per garantire a tutti gli incaricati il massimo aggiornamento in merito alle procedure operative ed alla prevenzione dei danni. I punti che seguiranno sono da intendersi come prerequisito fondamentale per l'ottimizzazione della gestione del Sistema Informativo Aziendale e la prevenzione di incidenti informatici. Il presente documento potrà essere soggetto a periodiche revisioni ed aggiornamenti che saranno opportunamente notificati a tutto il personale.

Utilizzo dell'elaboratore e della rete interna

L'accesso all'elaboratore, sia esso in rete o "stand alone", è sempre protetto da una o più password. La password assegnata non deve essere divulgata e deve essere custodita dall'assegnatario con la massima diligenza in ambiente protetto (cassetto con chiave per esempio). E' tassativamente proibito installare programmi "sprotetti" o senza licenza d'uso provenienti dall'esterno se non con l'autorizzazione esplicita dei contitolari (in quanto l'utilizzo di software non regolarmente acquistato dall'Istituto si configura come reato), anche in considerazione del grave pericolo di contrarre Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi.

Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup da parte dell'Amministratore del Sistema delegato (ivi compreso il monitoraggio dello spazio libero rimanente). Costituisce buona regola la periodica (consigliato mensilmente) pulizia degli archivi, con cancellazione di eventuali files obsoleti o inutili.

Particolare attenzione deve essere prestata alla duplicazione dei dati. E' infatti assolutamente da evitare una archiviazione ridondante che non consenta in modo chiaro ed inequivocabile l'identificazione dello stato di revisione di un documento. Il Personal computer deve essere spento ogni sera prima di lasciare gli uffici o va utilizzata la funzione di sospensione o stand by protetto da password.

E' evidente che 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, quindi si consiglia l'uso di screensaver con password.

Evenutali dispositivi personali quali notebook, pc personali, tablet sono autorizzati previa registrazione nella rete lan dell'Istituto nel limite di 1 a persona per anno scolastico.

Posta elettronica

L'utilizzo della posta elettronica contribuisce fortemente a rendere la comunicazione tempestiva, efficace ed economica. Il rispetto di alcune semplici regole può aiutare a migliorare ulteriormente l'utilizzo dello strumento.

La casella di posta del dominio istruzione.it deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti. E' buona norma compilare sempre il soggetto mittente ed evitare messaggi completamente estranei al rapporto di lavoro. E' possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario.

La consultazione della posta tramite web mail deve avvenire su sito https:// (funzione già attiva sul sito) e va disconnessa alla fine del suo utilizzo.

Utilizzo della rete Internet e dei relativi servizi

L'utilizzo imprudente di alcuni servizi della rete Internet, ancorché nell'ambito della normale attività professionale, può essere fonte di particolari minacce alla sicurezza dei dati e all'immagine dell'Istituto. Seguono alcune semplici regole che devono essere osservate in tale circostanza.

Navigazione *Internet*

L'utilizzo degli strumenti per la navigazione su Internet non è sottoposto ad alcun sistema automatico di controllo.

Rimane a disposizione dell'autorità giudiziaria, presso il provider telefonico, tutto il traffico internet generato dalla connessione disponibile presso l'Istituto. Tuttavia in casi di comprovata necessità tali sistemi potranno essere attivati. E' comunque necessario che vengano introdotte alcune limitazioni dettate da esigenze di Sicurezza, anche in considerazione del fatto che ogni singolo PC è caratterizzato da un indirizzo fisso che può, in determinate circostanze, causarne l'identificazione.

Dall'interno della rete aziendale, quindi:

è da evitare lo scaricamento di programmi software o quant'altro, anche gratuiti, se non per esigenze strettamente lavorative e professionali, considerando anche che il carico di downloading grava sulle spese dell'Istituto. (consumo di banda); è da evitare il frequente utilizzo di browser per navigazione internet e della posta elettronica del dominio istruzione.it se non per motivi strettamente lavorativi , di studio e ricerca professionale.

Documenti cartacei e archivi

Archivi centralizzati

Gli archivi centralizzati cartacei devono essere protetti in appositi armadi. Attreverso procedure automatizzate viene effettuata una **copia di backup giornaliera del server** in una unità esterna con partenza backup alle ore 23:30. In caso di progetti di "alto valore" è consigliabile effettuare, come azione preventiva supplementare, la masterizzazione su DVD o altro dispositivo removibile con frequenza settimanale o giornaliera (tramite richiesta all'amministratore di Rete delegato).

Via Domenico Cirillo, 33 – 70126 BARI / Tel. 0805421855 – 0805427938 – Fax 0805560784
Codice fiscale 93257010723 - E-mail: bavc010004@istruzione.it - PEC: bavc010004@pec.istruzione.it

Tutte le copie di sicurezza su supporti magneto–ottici devono essere consegnate all'amministratore di Rete delegato che provvederà alla custodia. Ogni qualvolta si procede alla masterizzazione, il collaboratore è tenuto a lasciarne traccia mediante apposita documentazione da consegnare all' Amministratore di Rete, riportante il proprio nome, cognome, data e ora della masterizzazione e relativa descrizione del contenuto.

Distruzione di documenti

Tutti i documenti contenenti dati personali o aziendali che si ritiene debbano essere eliminati devono essere distrutti e non gettati nei cestini.

E' vietato l'accumulo di documenti di qualsiasi genere negli ambienti di transito o pubblici, come per esempio corridoi, sale riunioni, atrio, stampanti, ecc.. esclusi i casi espressamente autorizzati o regolamentati.

Virus-Intrusioni

E' buona norma quella di controllare sempre la presenza dell'icona antivirus posizionata nella taskbar onde evitare attacchi di tipo virus sull'elaboratore. Qualora si presumi la presenza di virus sul proprio elaboratore, in caso di tentati accessi da parte di "esterni" (aule) o comunque in caso di anomalie generali, il collaboratore è tenuto ad informare celermente l'Amministratore di Rete delegato.

Riferimenti

Data Protection Officer: bavc010004@pec.istruzione.it