

Allegato 2 alla lettera di nomina Incaricato “Procedure Standard – Applicazione Misure Minime Sicurezza”

PROCEDURE STANDARD – MISURE MINIME DI SICUREZZA

DEFINIZIONE E GESTIONE DELLE USER ID

Autorizzazione informatica al trattamento

Gli Incaricati del trattamento sono autorizzati a livello informatico singolarmente o per gruppo di lavoro (definizione dei profili di accesso alle banche dati o applicativi che trattano dati).

Ogni user-ID deve identificare un unico utente

Per ogni computer e sistema di comunicazione l’user-ID deve identificare in modo univoco solo un utente. Le condivisioni o user-ID di gruppo non sono consentite.

Divieto di riutilizzo di user-ID

Per ogni computer e sistema di comunicazione, lo user-ID deve essere univoco e rimanere assegnato in modo permanente all’utente designato. Quando un dipendente o un Cliente terminano il loro rapporto di collaborazione con l’azienda, l’ID non deve essere riutilizzato.

Responsabilità degli utenti per tutte le attività riguardanti il proprio profilo

Gli utenti sono responsabili per tutte le attività riguardanti gli accessi eseguiti utilizzando il proprio profilo. Gli identificativi utente non possono essere utilizzati da nessuno tranne gli individui per i quali sono stati emessi. Gli utenti non devono permettere ad altri di effettuare alcuna attività con i loro profili, così come agli utenti è proibito svolgere attività con profili di altri utenti.

CRITERI OPERATIVI PER LA GESTIONE DELLE PASSWORD

I dati e le informazioni custodite nelle cartelle all’interno della rete aziendale, e a disposizione dell’intera struttura, costituiscono un patrimonio fondamentale ed indispensabile per garantire il normale svolgimento delle attività aziendali.

Tutti gli utenti possono accedere a queste cartelle e pertanto il loro stesso utilizzo deve avvenire in modo sicuro: è necessario che la connessione a tutte le postazioni sia protetta da password “resistenti”, in grado di preservare i dati contro possibili tentativi di accessi non autorizzati.

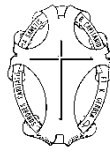
La procedura, quindi, ha lo scopo di definire i criteri minimi di protezione per regolamentare l’introduzione in azienda di password sicure nel rispetto della legge 196/2003.

Lunghezza minima delle password

Tutte le password utilizzate devono essere costituite da almeno 8 caratteri (o la massima lunghezza consentita dal sistema se non permette gli 8 caratteri)

Composizione delle password

Tutte le password saranno costruite con caratteri alfabetici e numerici. L’uso di caratteri non stampabili o inusuali è sconsigliato perché possono provocare inavvertitamente problemi di trasmissioni al network o richiamare non intenzionalmente funzioni di sistema.



Allegato 2 alla lettera di nomina Incaricato “Procedure Standard – Applicazione Misure Minime Sicurezza”

Password complessa

La composizione della password non può assolutamente basarsi su informazioni di carattere personale (nome di familiari, targa dell'auto, data di nascita, parte del proprio nome/cognome, luogo geografico di appartenenza non devono essere utilizzati). Non deve mai essere un acronimo o modo di dire comune.

Protezione della password

- La password non deve mai essere rivelata a nessuno e per nessuna ragione.
- Non devono essere utilizzate le funzioni di *Remember Password* presenti in diverse applicazioni (ad es. Outlook, Internet Explorer e Netscape Messenger).
- Non deve essere scritta o conservata in ufficio: in particolare non va archiviata in un file o in un qualsiasi supporto hardware (compresi i cellulari, i palmari e via dicendo), né scritta su fogli/post-it, agende, rubriche, ecc.
- Gli utenti non devono scrivere le loro password a meno che abbiano effettivamente nascosto la password in un numero di telefono o in altre sequenze di caratteri apparentemente senza correlazioni, o abbiano usato un sistema codificato per nascondere la password.

Divieto di riutilizzo di password già create in precedenza

Non deve essere riutilizzata una password già creata in precedenza.

Sostituzione autonoma della password

La password viene sostituita autonomamente dagli utenti, che ricevono una password temporanea alla prima connessione ma devono provvedere immediatamente alla sua modifica.

Scadenza della password

Gli utenti saranno obbligati anche alla modifica della password stessa alle scadenze previste, gestite automaticamente dal sistema: ogni 120 GIORNI sarà necessario modificare la propria password per garantirne la completa riservatezza.

PASSI OPERATIVI PER LA COSTRUZIONE DI UNA PASSWORD SICURA

Esempio:

La password può essere anche creata troncando frasi di senso compiuto quali ad esempio:

Sono andato al mare = SoAnAlMa ;

Tre più due fa cinque = 3p2Fcinque

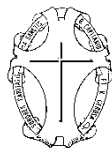
In pratica, mentre si ripete la frase la parola chiave esce da sola.

Avete creato una password di almeno 8 caratteri alfanumerica, la sua composizione non è basata su informazioni di carattere personale e non è presente in dizionari o dialetti.

UTILIZZO DELLA POSTAZIONE DI LAVORO

Accesso alla stazione di lavoro

- L'accesso alla stazione di lavoro deve avvenire utilizzando la propria password personale definita secondo quanto previsto dalla procedura Password sopra descritta.
- Non è consentito l'accesso alle stazioni di lavoro di colleghi né l'utilizzo di credenziali di altri.
- Il sistema operativo è configurato in maniera che l'utente si debba sempre identificare.



Allegato 2 alla lettera di nomina Incaricato

“Procedure Standard – Applicazione Misure Minime Sicurezza”

Divieto di installare/aggiornare software da parte degli utenti

- L'installazione di programmi è riservata ai Responsabili del sistema informativo ed è proibita ogni attività personale in questo senso.
- Sulla postazione di lavoro devono essere presenti solo i software standard aziendali. Qualsiasi altro tipo di software necessario per lavorare e non standard aziendale, deve essere approvato e installato da parte dei Responsabili del sistema informativo.
- Eventuali software non ritenuti di uso aziendale e tanto meno licenziati, verranno cancellati.

Gestione corretta della postazione di lavoro

- Gli utenti devono evitare di lasciare incustodite postazioni di lavoro con la sessione di lavoro aperta ed attiva (login effettuato).
- Gli utenti non devono lasciare visualizzate sulle postazioni di lavoro videate contenenti dati altamente riservati.

Custodia sicura dei supporti utilizzati per l'attività in azienda

Gli utenti non devono abbandonare incustoditi cd-rom, pen drive, cassette di backup, e/o tutto ciò che sia facilmente copiabile, asportabile ed occultabile.

Istruzioni sulle modalità di memorizzazione dei dati

Le informazioni conservate sulle unità di memoria locali delle workstation non saranno garantite da sistemi automatici di back-up, pertanto si prescrive di salvare tali dati in base alla procedura di back-up da effettuarsi su Cd o Memorie esterne.

GESTIONE ANTIVIRUS

Utilizzo di sistemi antivirus aggiornati

L'infrastruttura dell'azienda deve essere protetta con un sistema antivirus centralizzato o con programmi residenti sui singoli PC, e che il sistema o il singolo PC provveda automaticamente all'aggiornamento delle definizioni dei virus con frequenza quotidiana e automatica.

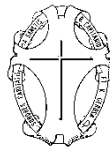
Controllo dei virus nei firewall, nei server e nei computer.

Un software antivirus deve essere installato e reso operativo su tutti i computer, i firewall, i server FTP, posta e intranet aziendale dell'azienda. L'aggiornamento delle definizioni dei virus deve essere effettuato automaticamente ogni qual volta si renda disponibile sul sito del produttore di software, e automaticamente diffuso a tutta la rete aziendale (server, client, ecc.)

UTILIZZO DELLA POSTA ELETTRONICA E INTERNET

L'infrastruttura di posta elettronica e di Internet è da ritenere a tutti gli effetti un bene aziendale. L'azienda sostiene i costi per l'utilizzo della banda assegnata, così come i costi per le operazioni di manutenzione ed amministrazione del patrimonio informativo.

Si richiede pertanto a tutti gli utenti aziendali, destinatari del presente regolamento, di utilizzare tali beni rispettando detto principio generale.



Allegato 2 alla lettera di nomina Incaricato

“Procedure Standard – Applicazione Misure Minime Sicurezza”

L'azienda non prevede un monitoraggio sistematico dell'utilizzo della rete da parte degli utenti e delle postazioni di lavoro, si riserva comunque il diritto di potersi assicurare dell'utilizzo corretto della propria infrastruttura da parte di tutti gli utenti aziendali e di perseguire eventuali comportamenti illeciti.

Detto regolamento si prefigge di definire le linee guida per un utilizzo appropriato della posta elettronica e di Internet rispetto a quanto definito dalla normativa vigente.

Autorizzazione all'uso personale del computer e dei sistemi di comunicazione

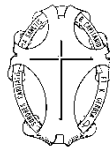
- L'azienda acconsente all'uso dei personal computer da parte degli utenti per scopi personali, quali l'invio di mail, la navigazione in Internet o la stampa di file, a condizione che tali attività non interferiscano con quelle lavorative e che rientrino in standard convenzionali di norme etiche e morali.
- È vietato collegarsi a siti quali le WebChat, i siti che propongono software protetto da copyright e attività illecite in generale. Tali siti, oltre a proporre argomenti contrari all'etica aziendale, sono spesso utilizzati come strumento per tentare di introdurre programmi pericolosi e virus nella rete aziendale.
- È vietato scaricare ed installare sulla propria postazione programmi non espressamente autorizzati dall'azienda. Tra i programmi devono considerarsi inclusi anche i sistemi di file sharing e gli screen saver, in quanto, oltre a non rispondere agli standard aziendali, possono essere un veicolo per l'introduzione di virus e possono rallentare le prestazioni del sistema sulla quale vengono installati.
- Si informano tutti gli utenti che i Sistemi Informativi utilizzeranno strumenti atti a verificare e registrare, a mezzo di analisi automatica, la presenza di eventuali comportamenti contrari alle politiche di utilizzo degli strumenti aziendali.

Regolamentazione della trasmissione di informazioni riservate

- I documenti e le comunicazioni trasmesse via e-mail sono leggibili da un'ampia categoria di persone e quindi questo canale di trasmissione, per quanto comodo, efficace e diffuso, deve essere considerato insicuro. È pertanto vietata la trasmissione via e-mail di documenti o di informazioni che possono essere considerate confidenziali.
- Nel caso sia comunque necessaria la trasmissione via e-mail di dati confidenziali si devono proteggere i documenti inserendo una password. Si consiglia comunque di non inviare documenti che superano i 5 MegaByte in quanto il destinatario potrebbe non riceverli. Si consiglia sempre la compressione dei documenti (Winzip).
- Non è consentita la trasmissione a mezzo di posta elettronica di dati sensibili, di alcun genere, salvo specifiche autorizzazioni da parte dei Sistemi Informativi, che avranno verificato preliminarmente le modalità di trasmissione.

Regolamentazione dell'uso della posta elettronica

- In rete circolano numerosi messaggi contenenti notizie false di allarmi o di appelli di cui si raccomanda di dare la massima diffusione. Questi messaggi non devono essere inoltrati. Nel caso sussista qualche dubbio contattare i Sistemi Informativi.
- È possibile ricevere messaggi, a volte in lingua inglese, da mittenti sconosciuti. In questo caso si deve procedere alla cancellazione del messaggio senza mai rispondere. Nel caso in cui il messaggio presenti un allegato questo NON dovrà essere aperto ma cancellato.
- Gli utenti non devono scaricare su disco allegati di posta elettronica di cui non si conosca con certezza il mittente o sulla sicurezza dei quali si nutrono anche minimi dubbi.



Allegato 2 alla lettera di nomina Incaricato “Procedure Standard – Applicazione Misure Minime Sicurezza”

SICUREZZA FISICA DEI DATI

L’accesso ad ogni ufficio, stanza dei computer e area lavorativa contenente dati sensibili deve essere fisicamente limitato.

I responsabili dello staff che lavora in queste aree devono consultare il responsabile della sicurezza per determinare il metodo appropriato di controllo di accesso (reception, serrature in metallo, serrature a chiave magnetica, ecc.).

Quando gli uffici non sono in uso, le porte devono essere chiuse a chiave.

Tutti i lavoratori che beneficiano di uffici personali devono chiudere a chiave le porte quando questi non sono in uso.

Benchè siano necessarie anche altre misure, questa pratica aiuterà a ridurre gli accessi non autorizzati a dati sensibili.

Tempi certi per il ripristino dei dati sensibili

Il ripristino dell’accesso ai dati in caso di danneggiamento degli stessi deve essere effettuato in tempi non superiori a sette giorni.