ASP PATRONATO
pei Figli del Popolo e Fondazione S.Paolo e S.Geminiano

REGOLAMENTO PER LA GESTIONE DEGLI STRUMENTI INFORMATICI

Sommario

Sistema di autenticazione e gestione delle credenziali

L'accesso agli strumenti elettronici, **aziendali e/o privati**, utilizzati per accedere al server e ai sistemi aziendali deve essere necessariamente subordinato ad un primo livello di procedure di autenticazione che deve prevedere l'inserimento da parte del dipendente/collaboratore di un proprio codice di identificazione (username) e di una parola chiave (password) riservata e conosciuta solamente dal medesimo.

Per l'accesso ai sistemi, ogni utente dispone di proprie credenziali che lo identificano in maniera univoca. La componente riservata delle credenziali di autenticazione (password) è definita ed elaborata rispettando i seguenti criteri:

- password note SOLO al dipendente/collaboratore
- composta da almeno 8 caratteri
- contenente le seguenti quattro caratteristiche:
    - lettere maiuscole (da A a Z)
    - lettere minuscole (da a a z)
    - numeri (da 0 a 9)
    - caratteri non alfanumerici (ad esempio !, ?, $)
- scadenza della password impostata a 6 mesi
- la nuova password impostata dall'utente non potrà essere uguale a quella in scadenza

Esiste inoltre un'autenticazione di secondo livello per l'accesso agli applicativi specifici regolato da un codice di identificazione proprio per ogni utente. Le password relative a tali sistemi di autenticazione sono formulate rispettando le regole sopra citate.

Ogni dipendente/collaboratore deve garantire tale livello di sicurezza, predisponendo, anche sui dispositivi personali utilizzati per finalità lavorative, la password così come imposta. In caso di violazioni causate da un mancato rispetto di tale procedura il Titolare potrà rivalersi nei confronti del dipendente/collaboratore stesso

Ulteriori policy di autenticazione per dispositivi mobili

Per l'accesso ai sistemi/software aziendali, tramite dispositivi mobili (smartphone e/o tablet) aziendali e/o personali, deve essere necessariamente attivato un sistema di autenticazione per lo sblocco dello schermo quali ad esempio: dato biometrico (impronta digitale) del dipendente/collaboratore (ad uso esclusivo personale, il Titolare non gestirà in alcun modo questi dati), password alfanumerica complessa, PIN numerico o tramite segno tracciato.

Con tale procedura viene protetto sia i dati contenuti nell'account di posta aziendale e gli eventuali documenti scaricati all'interno dei dispositivi mobili utilizzati.

Rischio di intrusione informatica esterna

Sistema di protezione Antivirus

Per evitare i danni derivanti dalla presenza di virus informatici sugli strumenti utilizzati (notebook, desktop, laptop, etc.) devono essere utilizzati appositi software antivirus, il cui scopo è proprio quello di rilevare la presenza di virus e contemporaneamente di bloccarli e quindi eliminarli dal sistema, riducendo allo stesso tempo il rischio che il virus possa cagionare danni al sistema, ai software installati ed accedere al server aziendale.

Il sistema di protezione antivirus deve coprire tutti i dispositivi utilizzati. L'antivirus deve possedere almeno le seguenti caratteristiche:

- Aggiornamento automatico, almeno quotidianamente
- Protezione in tempo reale
- Controllo della posta elettronica in entrata e in uscita

Firewall

Le connessioni tra i sistemi informatici e i server remoti devono utilizzare una VPN o una connessione criptata. Il collegamento a internet dei sistemi informatici deve avvenire attraverso un apposito firewall in grado di garantire un alto grado di sicurezza delle informazioni.

Aggiornamento periodico del software

Per i dispositivi deve essere garantito l'aggiornamento del sistema operativo e dei software utilizzati. Il sistema operativo deve essere aggiornato all'ultima versione disponibile (Windows 10 o MacOS Catalina).

Ripristino della disponibilità dei dati

Il dipendente/collaboratore dovrà lavorare sempre sul server aziendali, salvando direttamente i documenti sulle cartelle a ciò preposte, se ciò non fosse possibile per particolari esigenze lavorative o difficoltà momentanee occorre sempre garantire il backup dei documenti, con frequenza quotidiana, sul server aziendale, per evitare la perdita, anche accidentale, degli stessi.

Gestione dei dispositivi di memorizzazione esterni

Il dipendente/collaboratore deve assicurarsi che non rimangano incustoditi dati personali contenuti in supporti di memorizzazione (Hard disk, chiavette usb, memorie SD, CD/DVD, ecc.).

Per le unità esterne, il cui utilizzo non è di norma consentito, ma viene concesso per limitate necessità di trasferimento e di memorizzazione di dati, quando è strettamente necessario, occorre garantire che dopo tale utilizzo temporaneo il dipendente/collaboratore deve trasferire tali dati sui server aziendali, cancellarli dall'unità di memorizzazione esterna e, se possibile, formattare l'unità.

Se è necessario utilizzare dei dispositivi removibili per salvare documenti contenenti dati particolari occorre criptare il dispositivo, rendendo necessario l'inserimento di una parola chiave per poter accedere al contenuto dello stesso.

Conseguenza delle infrazioni disciplinari

Le infrazioni disciplinari alle indicazioni del presente documento potranno essere punite, a seconda della gravità delle mancanze, in conformità alle disposizioni di legge e/o del Contratto Collettivo Nazionale del Lavoro applicato, tra cui:

1. Il biasimo inflitto verbalmente;
2. Lettera di richiamo inflitto per iscritto;
3. Multa

Termine attività lavorativa/collaborazione

Al termine del periodo di lavoro o di collaborazione il dipendente/collaboratore dovrà eliminare tutti i collegamenti, gli accessi e le impostazioni implementate per attivare il servizio stesso

Clausola di riservatezza

Il dipendente/collaboratore si impegna a mantenere segrete e a non divulgare a terzi tutte le informazioni ricevute e messe a disposizione da ASP Minori per lo svolgimento delle attività lavorative.

Il dipendente si impegna altresì a non consegnare o divulgare a terzi, salvo il preventivo consenso scritto di ASP Minori, documentazioni e dati personali da quest'ultima consegnate, documenti interni aziendali, dati dei ragazzi/genitori e quant'altro presente nei server aziendali o negli strumenti online messi a disposizione per lo svolgimento delle attività lavorative.

Il dipendente/collaboratore si impegna a custodire con la massima diligenza tale materiale, al fine di tutelarne la riservatezza, e a non concederne accesso ad altri.

Il dipendente sarà personalmente responsabile per ogni atto di divulgazione a terzi di tale materiale non autorizzato espressamente per iscritto da ASP Minori.

In caso di inadempienza del dipendente agli obblighi assunti, ASP Minori avrà facoltà di far valer i propri diritti per il risarcimento dei danni subiti dalla violazione dei dati personali.

Accettazione

Con la firma del presente documento il dipendente/collaboratore accetta di rispettare tutte le disposizioni ivi contenute, senza nessuna esclusione.

Nome e Cognome (in stampatello)	Firma per esteso
_____	_____