IO 05.01 POLICY AZIENDALE PER LA SICUREZZA INFORMATICA

1. Scopo

La adozione diffusa delle nuove tecnologie informatiche ed in particolare il libero accesso alla rete Internet dai Personal Computer, espone l'Azienda a rischi di carattere patrimoniale, penale e reputazionale, nonché ai rischi connessi alla protezione dei dati personali, secondo quanto stabilito dal Regolamento (UE) 2016/679 (GDPR).
Premesso che l'utilizzo delle risorse informatiche aziendali deve sempre ispirarsi al principio della diligenza e correttezza, FORMODENA ha adottato il presente regolamento per contribuire alla diffusione della cultura della sicurezza ed evitare che comportamenti inconsapevoli inducano problemi o minacce alla sicurezza dei dati trattati e possano danneggiare l'azienda.
La presente policy ha come scopo la definizione delle condizioni per il corretto utilizzo degli strumenti informatici da parte di dipendenti e collaboratori.

2. Utilizzo delle dotazioni informatiche ricevute in assegnazione

Il Personal Computer, lo smartphone ed eventuali altri dispositivi informatici affidati al dipendente e/o collaboratore sono strumenti di lavoro. Ognuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione. Ogni utilizzo non inerente all'attività lavorativa può contribuire a provocare disservizi, costi e, soprattutto, minacce alla sicurezza. Perciò è opportuno seguire alcune semplici ma importanti regole di comportamento:

– Non è consentita l'attivazione della password d'accensione (BIOS)
– Non è consentito all'utente modificare le caratteristiche hardware e software impostate sul proprio dispositivo.
– I dispositivi devono essere spenti prima di lasciare il proprio ufficio, sia per motivi di sicurezza che di risparmio energetico.
– Ogni evento accidentale che causi una rottura o comunque una non disponibilità della dotazione deve essere tempestivamente segnalato ai responsabili ICT.
– Le informazioni archiviate devono essere esclusivamente quelle necessarie all'attività lavorativa
– L'utente deve lavorare e quindi salvare i dati e le informazioni necessarie all'attività lavorativa sui server aziendali che effettuano backup dei dati
– La tutela della gestione locale di eventuali dati su postazioni di lavoro personali - personal computer che gestiscono localmente documenti e/o dati - è demandata all'utente finale e non sono soggetti a backup dei dati.
– L'impossibilità di effettuare copia in rete (es. lavoro continuativo fuori sede) deve essere segnalata al servizio IT che provvederà idonei sistemi di tutela dei dati aziendali (es. siti documentali dedicati accessibili tramite Internet).
– Se non autorizzato e abilitato dal servizio ICT, è vietato l'utilizzo di supporti di archiviazione removibili (USB e Hard Disk esterni) per la memorizzazione dei dati aziendali. Qualora sia necessario utilizzarli, i dati contenuti dovranno essere crittografati con i software appositi, secondo le indicazioni del servizio ICT.
– Le gestioni esclusivamente locali (cioè solo sul proprio computer) di dati o documenti non sono ammesse: la gestione centralizzata su Server è una garanzia necessaria per il lavoro dell'Azienda che deve poter disporre in qualsiasi situazione delle proprie informazioni: l'utente finale è responsabile della perdita di dati e documenti nel caso di non ottemperanza al salvataggio in rete.
– Non è consentita l'installazione di programmi diversi da quelli autorizzati e predisposti dal servizio ICT.
– Non è consentita (per legge) la riproduzione o la duplicazione di programmi informatici né lo scaricamento di contenuti in palese violazione dei diritti d'autore.
– Gli operatori tecnici dell'ICT aziendale possono in qualunque momento procedere alla rimozione di file o applicazioni ritenuti pericolosi per la sicurezza della rete aziendale.

3. Utilizzo della rete aziendale

L'accesso alla rete aziendale è protetto da password; per l'accesso deve sempre essere utilizzato il proprio profilo personale composto da username per il login e relativa password.
Per la sicurezza aziendale non è permesso:

– Utilizzare la rete aziendale e le sue risorse per fini non autorizzati o comunque non lavorativi.
– Connettere in rete postazioni di lavoro private o non assegnate dall'Azienda se non dietro esplicita e formale autorizzazione del responsabile IT aziendale.
– Organizzare cartelle private condivise in rete sia dotate di password, sia sprovviste di password se non dietro esplicita e formale autorizzazione del responsabile IT aziendale.
– L'installazione non autorizzata di modem esterni (es. modem 4G USB, Smartphone privato, router wireless) che sfruttino il sistema di telefonia mobile per l'accesso a Internet.
– L'introduzione di qualsiasi apparato di rete non fornito dall'azienda (ad esempio unità di storage, access point, trasmettitori audio/video, media player o altro).
– Non fornire a personale esterno le password di collegamento alle reti WIFI aziendale e mobile, fornire a ospiti e studenti la password solo della rete ospiti/guest

4. Gestione delle password

Le password d'ingresso alla rete, di accesso ai vari programmi in rete per i trattamenti dei dati e ad Internet, sono attribuite dal servizio ICT.
Al riguardi qualsiasi richiesta relativa a Concessione/Revoca/Modifica delle abilitazioni applicative deve essere veicolata tramite il sistema di IT aziendale. L'utente è tenuto a conservare nella massima segretezza la parola di accesso alla rete ed ai sistemi e qualsiasi altra informazione legata al processo di autenticazione.
L'utente è tenuto a bloccare il proprio computer ogni qualvolta si assenti dall'ufficio nel quale è ubicata la postazione di lavoro: la responsabilità di un eventuale utilizzo indebito della postazione è dell'utente che ha lasciato aperto e disponibile il proprio account.
La password deve essere immediatamente sostituita, nel caso si sospetti che la stessa abbia perso il requisito della segretezza e comunque ogni 120 giorni
Le credenziali e/o le password aziendali non devono in alcun modo essere utilizzate per servizi Internet estranei all'Azienda (es. blog, social network, servizi email esterni, etc)

5. Utilizzo di dispositivi portatili

L'utente è responsabile dei dispositivi portatili (es. pc e smartphone)l assegnatogli dall'Azienda e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo sul luogo di lavoro.
Ai PC portatili si applicano le regole dl utilizzo previste per i PC connessi in rete con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
I dispositivi portatili utilizzati all'esterno del perimetro aziendale, in caso di allontanamento, devono essere custoditi in un luogo protetto. Ogni evento accidentale, furto o rottura del bene, deve essere tempestivamente segnalato al diretto responsabile ed all'ICT. **La tempestività è resa particolarmente necessaria per effetto di quanto previsto dal vigente GDPR all'art. 33 (comunicazione di data breach entro 72 ore).**
Nel caso di accesso alla rete aziendale tramite VPN utilizzare l'accesso in forma personale e custodire le proprie credenziali in modo rigoroso. Collegarsi periodicamente alla rete interna per consentire il caricamento degli aggiornamenti di sistema e antivirus.
Per l'accesso alla VPN è stato adottato un sistema di collegamento con MFA (con OTP generata da Microsoft Authenticator) al fine di garantire un accesso protetto alla rete aziendale.

6. Uso della posta elettronica e sistemi di messaggistica

L'abilitazione alla posta elettronica avviene all'ingresso in Azienda di ogni nuovo dipendente o collaboratore. La casella di posta personale, assegnata dall'Azienda all'utente, è uno strumento di lavoro.
L'indirizzo di posta elettronica aziendale nominativo (es. mario.rossi@formodena.it) prevede delle password di accesso all'account che non possono essere diffuse a terzi. E' vietata la consultazione e l'utilizzo della posta elettronica di altri utenti.
Non é consentito consultare gli account di posta personali attraverso i computer aziendali e soprattutto è rigorosamente proibito - per i gravi rischi possibili - scaricare allegati dalla propria posta personale.

Al sensi di legge, ogni utente è responsabile del corretto utilizzo della propria casella email. Nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus occorrerà cancellare i messaggi senza aprire gli allegati. Nel caso di messaggi provenienti da mittenti conosciuti ma che contengono allegati sospetti (file con estensione .exe .scr .pif .bat .cmd ,vbs .dll .js .vbs o file compressi .zip .rar .7z contenenti file come le estensioni precedenti), questi ultimi devono essere verificati attentamente se necessario con l'ausilio del servizio IT, prima di essere aperti.
L'invio di allegati pesanti è limitato dal sistema a 15MB, ma è possibile caricare file pesanti nel proprio Google Drive aziendale e da lì condividerli in posta elettronica.
Il sistema di posta non deve essere utilizzato per l'invio massivo di file e di grandi quantità di dati: richiedere il supporto IT per tali necessità di trasferimento in rete.
Nel caso di debba inviare un documento esterno dell'Azienda è preferibile utilizzare il formato PDF.
L'iscrizione a "mailing list" esterne è concessa solo per motivi professionali, prima di iscriversi occorre verificare se l'organizzazione sia affidabile.
La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti, ove già scaricati ed archiviati.
E' necessario controllare periodicamente la cartella SPAM / POSTA INDESIDERATA, per verificare che non ci siano finiti dentro messaggi importanti.
Anche in altri sistemi di messaggistica, come ad esempio WhatsApp, valgono le stesse regole comportamentali per la sicurezza e l'etica aziendale.

7. Uso della rete Internet e del relativi servizi

L'abilitazione ad Internet è predisposta per ogni postazione e utenza aziendale.
Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. È proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa. Non possono essere utilizzati modem privati per il bypass delle sicurezze aziendali e il collegamento autonomo alla rete Internet.
Per ragioni di sicurezza, è fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal servizio ICT.
E' vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati) e di bacheche elettroniche.
La rete Internet è una preziosa risorsa aziendale: è vietato l'utilizzo indiscriminato della banda in particolare per traffico streaming (audio/video) e download massivi.
I sistemi di controllo aziendale eseguono un monitoraggio continuo delle risorse di banda al fine di individuare ogni abuso. A salvaguardia dell'integrità e disponibilità delle risorse di rete, il servizio ICT può decidere di bloccare l'accesso a quelle determinate risorse in rete qualora rilevi utilizzi non conformi alla presente policy.
Salvo diversa indicazione, non è consentito sincronizzare o copiare documenti aziendali dal proprio PC su servizi cluod esterni al perimetro della rete aziendale (es. Dropbox, Google Drive, etc.).

8. Protezione antivirus

Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo (ad esempio non aprire mail o relativi allegati sospetti, non navigare su siti non professionali ecc.)
Ogni utente è tenuto a controllare la presenza e il regolare funzionamento del software antivirus aziendale, non ostacolarne l'aggiornamento, né le scansioni automatiche periodiche. Nel caso che il software antivirus rilevi la presenza di un virus che non è riuscito a ripulire, l'utente dovrà immediatamente sospendere ogni elaborazione in corso spegnendo il dispositivo e segnalare l'accaduto al responsabile ICT.
Ogni supporto dati di provenienza esterna all'azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo. Qualsiasi incertezza o sospetto relativi a documenti o supporti può essere risolta rivolgendosi al personale competente del servizio ICT.