ALLEGATO C

Istruzioni Operative: Lavoro agile – politiche di sicurezza sul corretto utilizzo dei dispositivi mobili

Redatto da	Referente Gruppo di lavoro		
		Firma	*data*
Verificato da	Responsabile Sistemi Informatici e Transizione all'Amministrazione Digitale		
		Firma	*data*
Approvato da	Direttore Amministrativo		
		Firma	*data*

STORIA DELLE MODIFICHE APPORTATE

Data	Rev.	Motivo del cambiamento
Gennaio 2023	00	Prima emissione

DEFINIZIONI E ABBREVIAZIONI

AOPG: Azienda Ospedaliera di Perugia

Chiavetta USB: o unità flash USB o penna USB (anche in inglese USB flash drive, o pendrive) è una memoria di massa portatile di dimensioni molto contenute che si collega al computer mediante la porta USB.

Dati: l'insieme di informazioni di cui un dipendente o un collaboratore (a prescindere dal rapporto contrattuale con l'Azienda) può venire a conoscenza e di cui deve garantire la riservatezza e la segretezza e non solo i "dati personali" intesi a norma di legge

Dati personali: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (art. 4 GDPR);

Device (dispositivo): personal computer e altre unità hardware quale periferica/dispositivo elettronico, anche ad alta tecnologia e di piccole dimensioni (smartphone, e-book reader, tablet PC ecc.).

Dipendente: personale dell'ente assunto con qualsiasi tipo di forma contrattuale, anche in stage o tirocinio.

Disciplinare Aziendale: "Disciplinare per il corretto utilizzo degli strumenti informatici, telematici, Internet e Posta Elettronica" (approvato con Delibera del Direttore Generale n. 493/2019), revisionato nell'agosto 2020 (AzOsp_ManOp_13 Rev.1) disponibile sul portale Aziendale

File: porzione di memoria (fissa o mobile) che contiene un insieme organizzato di informazioni omogenee.

GDPR: General Data Protection Regulation - Regolamento Generale sulla Protezione dei Dati - Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016

Malware: abbreviazione per malicious software (che significa letteralmente software malintenzionato, ma di solito tradotto come software dannoso), indica un qualsiasi programma informatico usato per disturbare le operazioni svolte da un computer, rubare informazioni sensibili, accedere a sistemi informatici privati, o mostrare pubblicità indesiderata

NIS: Network Information Security – Direttiva Europea che definisce gli standard di sicurezza informatica per gli asset strategici di una nazione, in particolare per gli OSE (Operatori di Servizi Essenziali)

Postazione di lavoro: luogo attrezzato per svolgere un'attività lavorativa dotato di personal computer ed eventuali altre unità hardware.

Rete locale: una Local Area Network (LAN) (in italiano, rete locale) è una rete informatica di collegamento tra più computer, estendibile anche a dispositivi periferici condivisi, che copre un'area limitata, come un'abitazione, una scuola, un'azienda o un complesso di edifici adiacenti.

Virus: programma appartenente alla categoria dei malware che, una volta eseguito, infetta dei file in modo da arrecare danni al sistema, rallentando o rendendo inutilizzabile il dispositivo infetto.

PREMESSA

Il presente documento nasce dall'esigenza dell'Azienda di ridurre al minimo i rischi di sicurezza informatica associati agli accessi dall'esterno del perimetro della rete locale (LAN), oltre a tutelare il patrimonio di dati trattati dall'Azienda.

Con il recepimento della Direttiva Europea NIS (Network Information Security), AOPG ha l'obbligo di innalzare i livelli di sicurezza informatica per garantire la protezione dei dati personali dei propri dipendenti e dei cittadini che usufruiscono dei servizi erogati dall'Azienda. Nel rispetto sia di tale normativa, sia del Regolamento Europeo per la Protezione dei Dati Personali (GDPR).

I dispositivi portatili ed i dati in essi contenuti stanno diventando un obiettivo sempre più comune per i criminali, non solo criminali informatici (cosiddetti hacker) ma vere e proprie organizzazioni volte all'estorsione, allo spionaggio o al terrorismo.

In caso di furto, oltre all'impatto finanziario derivante dalle spese relative alla loro sostituzione, vi sono dei costi tangibili "nascosti" associati, soprattutto, alla reputazione e alla privacy personale associati alla perdita di informazioni sensibili, aziendali o personali anche insostituibili, gestite in tali dispositivi. La perdita rappresentata, sebbene difficile da valutare, rappresenta un elevato costo per AOPG. Siccome ognuno di questi dispositivi potrà contenere informazioni personali, dal punto di vista della sicurezza viene considerato alla stregua di un computer desktop aziendale.

CAMPO DI APPLICAZIONE

Gli standard di sicurezza descritte nel presente documento si applicano a tutti i dipendenti di AOPG che aderiscono al progetto denominato "Smart Working" e che utilizzano un pc portatile di proprietà dell'Azienda oppure usufruiscono del proprio pc portatile personale o device mobile, opportunamente configurato per accedere in sicurezza ai servizi informatici aziendali.

Il disciplinare si applica a tutti i dipendenti, senza distinzione di ruolo o livello, nonché a tutti i collaboratori dell'Azienda Ospedaliera di Perugia a prescindere dal rapporto contrattuale con la stessa intrattenuto (es. collaboratori esterni, Co.co.co., collaboratori a progetto, stagisti, medici in formazione, borsisti ecc.), di seguito "utenti".

MODALITA' OPERATIVE

Istruzioni per la custodia degli strumenti per lo Smart Working

Per il corretto utilizzo dei dispositivi aziendali, forniti da AOPG, si rimanda al Disciplinare Aziendale (AzOsp_ManOp_13 Rev.1). L'accesso tramite il dispositivo portatile è consentito al dipendente AOPG nei seguenti casi:

- Internamente all'Azienda, utilizzando la rete di dominio aziendale, cavo o Wi-Fi;
- Dall'esterno di AOPG, dal proprio domicilio utilizzando il collegamento Internet domestico;
- Esternamente ad AOPG in mobilità, utilizzando la rete mobile (cellulare) o Wi-Fi di fornitore noto.

NB: La connessione ad una rete cavo o Wi-Fi pubblica, non conosciuta, quale ad esempio la rete di un hotel o di un locale pubblico, è da evitare in ogni caso, poiché comporta gravi rischi di sicurezza, come il furto delle credenziali dell'utente e l'intercettazione di tutte le informazioni trasmesse e gestite tramite il dispositivo.

I PC portatili e i device mobili sono anche particolarmente vulnerabili alla perdita e al furto. Criminali singoli e organizzati possono commettere il furto sia all'interno degli edifici di AOPG che esternamente all'Azienda. Il rischio è potenzialmente maggiore durante gli spostamenti e quando si viaggia, specialmente se il dipendente AOPG si trova in un ambiente non familiare o si sta concentrando sul viaggio stesso.

Nonostante nella maggior parte dei casi il malvivente tragga profitto dalla vendita del pc portatile sul mercato nero, esiste un numero crescente di criminali che ruba questi dispositivi specificamente per i dati sensibili che possono contenere. Tali informazioni, se rivelate, potrebbero causare danni relativi alla privacy, imbarazzo, perdita di reputazione o significativi effetti finanziari o commerciali per APSS.

Nel contesto lavorativo di AOPG, generalmente le informazioni trattate possono comprendere:

- dati personali sanitari di assistiti e pazienti, informazioni personali relative ai dipendenti;
- qualsiasi informazione personale e privata dell'utente che vorrebbe mantenere privata;
- note di ricerca, dati e informazioni commercialmente sensibili, dati di proprietà intellettuale;
- dati finanziari ed economici.

Per contrastare questi rischi, la sicurezza dei dispositivi mobili viene affrontata in cinque modalità:

a. educazione dell'utente attraverso una maggiore responsabilità e consapevolezza dei rischi e dell'applicazione di una politica di sicurezza dei pc portatili, attraverso la partecipazione ai corsi in "Competenze Digitali in Sanità" organizzati annualmente da AOPG;

b. sicurezza fisica dell'ambiente in cui è custodito o si utilizza il dispositivo portatile, sia all'interno di strutture AOPG, al proprio domicilio che in viaggio;
c. controllo sicuro dell'accesso al dispositivo portatile mediante autenticazione con password sufficientemente robusta (nel rispetto del Disciplinare Aziendale);
d. protezione dei dati conservati sul dispositivo mediante backup e crittografia;
e. tracciamento / cancellazione dei dati, in particolare per i dispositivi ad alto rischio o contenenti dati molto sensibili.

In ogni caso, per limitare danni e perdite di informazioni, si consiglia la minimizzazione della memorizzazione dei dati aziendali sul disco fisso del dispositivo portatile, sia in termini di dimensioni che di tempo.

Al di fuori delle strutture di AOPG, è vivamente sconsigliata la stampa su carta di informazioni aziendali.

Per evitare il furto del dispositivo portatile si consiglia di elevare al massimo il grado di attenzione durante gli spostamenti, sia internamente ma soprattutto al di fuori delle strutture AOPG.

Nel caso in cui si stia lavorando in condizioni di precaria connettività dati dal punto di vista della qualità e continuità del servizio, ad esempio durante un viaggio in treno, è permesso scaricare sul disco locale del dispositivo portatile il documento di lavoro per elaborarlo in modalità offline. A connettività ripristinata, si dovrà copiare il documento nella cartella aziendale, e si dovrà cancellare il documento stesso dal disco locale del dispositivo.

Configurazione dei dispositivi aziendali per lo Smart Working

Le politiche applicate alle postazioni di lavoro aziendali si applicano anche ai dispositivi portatili. Tra queste regole, elencate nel Disciplinare Aziendale, ricordiamo la necessità per tutti gli utenti di accedere alla rete aziendale mediante le credenziali personali, il cambio della password almeno una volta ogni tre mesi o in tutti i casi in cui si ritenga che sia stata inavvertitamente divulgata o compromessa e il logoff automatico dei programmi.

Gli utenti solitamente non dispongono dell'autorizzazione per installare il software o modificare le configurazioni del pc portatile. Tuttavia, la configurazione e l'installazione di particolare software va espressamente richiesta ai Sistemi Informatici tramite il portale Segnalazioni online.

In nessun caso il personale non autorizzato potrà eseguire operazioni di modifica della configurazione dei dispositivi.

Al fine di proteggere le informazioni memorizzate nei portatili, AOPG ha installato un sistema di crittografia del disco che, in caso di tentativi di accesso con password diverse da quella aziendale, rendono illeggibile l'intero contenuto.

Il pc portatile e il device portatile sono abilitati per lavorare in maniera "Smart" tramite la configurazione di tutti i software e i collegamenti necessari.

Utilizzo di dispositivi personali per lo Smart Working

AOPG concede di utilizzare per fini lavorativi il proprio PC portatile o device personale tramite accesso VPN alla rete aziendale. Queste modalità di accesso mettono in sicurezza il transito dei dati sulla rete, ma non sono sufficienti ad eliminare il rischio di violazioni sui dati personali come il furto delle credenziali di autenticazione, la modifica dell'integrità e la diffusione di dati personali. AOPG, infatti, non possedendo il controllo sugli strumenti personali dell'utente, non è in grado di assicurare la sicurezza locale di tali dispositivi, e conseguentemente non può garantire che questo rischio sia ridotto.

È requisito essenziale che i dati abbiano lo stesso livello di sicurezza di quando sono trattati con gli strumenti aziendali messi a disposizione dall'Azienda. Pertanto, l'utente deve provvedere a configurare i propri dispositivi personali con un alto livello di sicurezza, indipendentemente dal tipo di sistema operativo utilizzato, marca e modello del personal computer o del dispositivo mobile.

Al fine di non incorrere in situazioni di vulnerabilità, con conseguenti rischi di violazioni sui dati, l'utente dovrà implementare, a sue spese e sotto la sua responsabilità, le seguenti misure di sicurezza tecniche e comportamentali:

a. verificare costantemente che il proprio personal computer o dispositivo mobile possieda un sistema operativo aggiornato ed applicare costantemente gli aggiornamenti di sicurezza resi disponibili dal produttore;

b. verificare costantemente che sul sistema sia installata una soluzione antivirus e anti-malware di mercato funzionante ed aggiornata, con caratteristiche di protezione in tempo reale dalle minacce, aggiornamenti automatici e scansioni programmate;

c. applicare costantemente gli aggiornamenti di sicurezza di tutte le applicazioni installate sul personal computer o dispositivo personale;

d. verificare costantemente che sul sistema non siano presenti software non conformi o malevoli. In caso contrario, l'utente dovrà provvedere alla loro immediata rimozione.

Si ricorda inoltre che:

- Di norma, i dati aziendali non devono essere memorizzati sul disco locale del personal computer o del dispositivo, né su chiavette USB o dischi esterni di memorizzazione, né su servizi di cloud storage personali;

- se, per motivi di continuità operativa, l'utente dovesse salvare dei dati sui sistemi di memorizzazione non conformi a quanto raccomandato ai punti precedenti, una volta reinseriti e salvati nel sistema gestionale o nell'applicativo aziendale tali dati andranno cancellati dai sistemi di memorizzazione non conformi;

- in caso di contenzioso o indagini dovute a violazioni sui dati aziendali e/o illeciti, l'utente dovrà mettere a disposizione degli inquirenti, per le opportune verifiche sullo stato di sicurezza e sui dati in esso contenuti e per tutto il tempo necessario, il proprio personal computer portatile o dispositivo personale utilizzato per lo Smart Working.

Gestione del rischio

La politica aziendale è quella di consentire al personale di utilizzare i dispositivi portatili come aiuto nello svolgimento del proprio lavoro. I rischi associati a questo utilizzo sono gestiti con le seguenti attività:

- Applicazione di controlli tecnologici come l'accesso con autenticazione forte e il cambio periodico della password;

- controllo antivirus e anti-malware per proteggere i programmi e l'accesso alle informazioni sui dispositivi;

- sul pc portatile di proprietà aziendale, limitazione dei privilegi di accesso in modo che l'utente non possa installare software non aziendale;

- assistenza e formazione agli utenti a comprendere i rischi connessi all'uso di questi dispositivi e come possano essere mitigati al meglio

Rimane responsabilità dell'utente mantenere protetto e custodire il dispositivo, sia aziendale che privato, secondo le politiche di sicurezza contenute in questo documento ed attuare le generali e comuni misure di sicurezza tecniche e comportamentali nell'utilizzo dei dispositivi mobili.

Segnalazione di furto

In caso di furto del dispositivo, sia aziendale che personale, l'utente dovrà denunciare prontamente l'accaduto al Posto Fisso di Polizia o al più vicino commissariato, inviando copia della denuncia ai Sistemi Informatici e Transizione all'Amministrazione Digitale.

RIFERIMENTI NORMATIVI E BIBLIOGRAFIA ESSENZIALE

General Data Protection Regulation - Regolamento Generale sulla Protezione dei Dati - Regolamento (EU) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016

Network Information Security – Direttiva Europea (UE) 2016/1148 sulla sicurezza delle reti e dei sistemi informativi

Decreto Legislativo 18 maggio 2018, n. 65 - Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.