LINEE GUIDA PER LA SICUREZZA DELL'ACCESSO AI DATI INFORMATICI

CORRETTO UTILIZZO DELLE WORKSTATION E DEI PC PORTATILI

L'utente che ha disposizione l'accesso a una workstation o un pc portatile, ha il dovere di utilizzare la macchina solo ed esclusivamente per lo scopo per cui gli è stata affidata. Inoltre i dispositivi informatici sono strumenti di lavoro appartenenti al patrimonio aziendale e per questo devono essere utilizzati per fini professionali (ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza).

Il Personal Computer (PC) è uno strumento di lavoro affidato al Dipendente, di cui lo stesso è responsabile sia per la parte Hardware che Software. Il PC deve essere utilizzato per i soli ambiti inerenti all'attività lavorativa; eventuali informazioni salvate -anche temporaneamente- sulla postazione di lavoro, devono pertanto riguardare esclusivamente la propria attività lavorativa. Ogni utilizzo del PC non afferente alla propria attività lavorativa può contribuire ad innescare disservizi, costi di assistenza e manutenzione e, soprattutto, minacce alla sicurezza dell'intera rete aziendale e/o delle reti telematiche e dei sistemi informatici di terzi esponendo l'organizzazione e gli stakeholder aziendali a crimini informatici.

Tutti i dipendenti della Casa di Cura Villa Esther sono a conoscenza che i dati conservati nel proprio Personal Computer, compresi i messaggi di posta elettronica in entrata e in uscita, possono essere visionati dai Responsabili della struttura in caso di necessità dovute a titolo esemplificativo e non esaustivo, a malfunzionamenti del sistema, esigenze lavorative, assenza dell'Incaricato, ecc... I Responsabili di struttura, pertanto, per l'espletamento delle loro funzioni, hanno la facoltà in qualunque momento di accedere ai dati trattati dai propri collaboratori, ivi compresi gli archivi di posta elettronica in entrata ed uscita, chiedendo formalmente accesso alla struttura I.T. Per cui sono assolutamente vietai comportamenti atti a vietare tali accessi (archivi protetti da password, crittografati, etc.). Nel caso in cui l'utente sia costretto ad assentarsi dal locale in cui è ubicata la stazione di lavoro o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima è tenuto ad eseguire una delle seguenti operazioni: spegnimento, blocco o disconnessione dalla sessione di lavoro. Ad ogni modo, sulle postazioni di lavoro (fisse e laptop) è stata implementata una policy che prevede il blocco automatico della postazione dopo alcuni minuti di inattività e che richiede di nuovo l'accesso con password.

UTILIZZO DELLE CREDENZIALI DI AUTENTICAZIONE

L'accesso all'elaboratore è protetto da codice identificativo e password (credenziali), che devono essere custoditi con la massima diligenza e non divulgate, né trascritte su mezzi facilmente accessibili. Le credenziali di autenticazione per l'accesso ai dispositivi ed alla rete vengono predisposte dagli amministratori della struttura I.T. all'atto dell'assunzione del nuovo dipendente in seguito a confacente comunicazione della struttura Politiche e Gestione Risorse Umane e devono essere obbligatoriamente modificate al primo accesso. La password di accesso alla rete ha un periodo di validità limitato; ad intervalli regolari verrà quindi richiesto all'utente di modificare la password. La password scelta non deve contenere riferimenti agevolmente riconducibili all'Autorizzato, deve essere modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. L'utente non può riutilizzare una password già utilizzata. In caso di estinzione del rapporto contrattuale con l'Incaricato, la struttura Gestione Risorse Umane ne dà tempestiva comunicazione alla struttura I.T. e questi provvede ad inibire l'accesso alle postazioni entro tre giorni lavorativi dal ricevimento della comunicazione (o non appena ne venga a conoscenza).

CREDENZIALI DI ACCESSO AI SERVIZI E AGLI APPLICATIVI

L'Utente che lavora sulla singola macchina potrà gestire ulteriori password legate a software gestionali. Sebbene tali software siano dati in concessione d'utilizzo o completamente esternalizzati e il reparto I.T. non abbia alcun controllo su di essi, la Casa di Cura Villa Esther garantisce che le policy di sicurezza ed accesso garantite del fornitore siano completamente compatibili con l'utilizzo aziendale e con le norme presenti in tale documento.

Per cui a titolo esemplificativo, anche per questi software l'utente ha la facoltà e l'obbligo di monitorare le credenziali seguendo le regole già descritte. Più in generale, l'utente che ha la facoltà di accesso a tali software è tenuto a rispettare le norme e i comportamenti sopra descritti per l'accesso ai dispositivi.

CORRETTO UTILIZZO DELLE CREDENZIALI

Gli utenti sono responsabili della custodia e dell'utilizzo delle proprie credenziali di autenticazione; la password, formata da lettere (maiuscole e minuscole), numeri e/o caratteri speciali, nei limiti consentiti dai sistemi, deve avere le seguenti caratteristiche:

- deve essere di lunghezza non inferiore ad 8 caratteri oppure, nel caso in cui ciò non sia possibile, da un numero di caratteri pari al massimo consentito dal connesso applicativo;
- deve essere composta da caratteri maiuscoli, caratteri minuscoli, numeri e caratteri speciali (es.Hatv%67g);
- non deve contenere riferimenti agevolmente riconducibili all'Incaricato o ad ambiti noti;
- deve essere obbligatoriamente cambiata al primo utilizzo e successivamente ogni 180 giorni (per quanto concerne le credenziali di dominio esiste un meccanismo di scadenza automatica);
- deve essere diversa dalle ultime 10 password precedentemente utilizzate;
- non deve essere basata su nomi di persone, date di nascita, animali, oggetti o parole ricavabili dal dizionario (anche straniere), o tratta da informazioni personali;
- non deve presentare una sequenza di caratteri identici o in gruppi di caratteri ripetuti;
- non deve essere memorizzata in funzioni di log-in automatico, in un tasto funzionale o nel browser utilizzato per la navigazione Internet;
- deve essere annullata e sostituita con una nuova - per motivate necessità di urgente accesso alle informazioni ed impedimento del titolare delle credenziali - da parte degli amministratori dei servizi o loro delegati. In questo caso essa dovrà essere nuovamente modificata al primo accesso da parte dell'Incaricato.

Qualora le limitazioni tecniche del sistema non permettano la configurazione dello stesso al fine di limitare selettivamente l'utilizzo di password "robuste", sarà onere dell'utilizzatore l'impostazione di password secondo le specifiche in precedenza elencate.

L'utente si impegna a non cedere a terzi le proprie credenziali di accesso alla rete, consapevole che la cessione delle stesse consente ad altri l'accesso e l'utilizzo dei relativi servizi, ovvero l'accesso ai dati cui il soggetto è abilitato con conseguenze quali la visualizzazione di informazioni riservate, la distruzione e/o modifica di dati.

È assolutamente proibito accedere alla rete e ai programmi con delle credenziali di autenticazione, in particolare con un codice d'identificazione utente, diverso da quello assegnato. La responsabilità di qualsiasi azione svolta dopo aver eseguito la procedura di autenticazione sarà attribuita all'utente assegnatario delle credenziali. L'utente è quindi responsabile, sia nei confronti dell'Azienda che di terzi, di fatti e atti illeciti, con particolare riferimento all'immissione in rete di contenuti critici o contrari all'ordine pubblico o al buon costume così come definiti dalla giurisprudenza corrente.

È fatto divieto annotare la password su supporti facilmente rintracciabili (quali post-it, quaderni, ecc…) e, soprattutto, in prossimità della stazione di lavoro utilizzata.

L'utente si impegna a modificare tempestivamente la password d'accesso alla rete qualora tale dato sia stato rubato, smarrito, o sia noto a terzi, dandone comunicazione alla struttura I.T. L'Azienda si fa garante della custodia dei dati personali forniti dall'utente e si impegna a non rivelarli a terzi, se non a fronte di legittima richiesta da parte di Autorità Giudiziaria, Autorità di Pubblica Sicurezza e Garante per la Protezione dei Dati Personali.

CREDENZIALI AMMINISTRATIVE

I privilegi di amministrazione sono limitati ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi previa nomina formale ad "Amministratori di Sistema". Laddove il sistema lo permetta, i permessi amministrativi saranno concessi in maniera granulare per consentire unicamente l'evasione delle attività elencate nell'ambito di operatività per cui l'amministratore è stato nominato.

Nella Casa Di Cura Villa Esther non è previsto *l'inventario delle utenze amministrative* sono invece state consegnate all'amministratore unico e al DPO una busta chiusa con le credenziali di accesso con potere amministrativo per il solo Domain Controller.

UTILIZZO E CUSTODIA DI PEN-DRIVE, CD DATI E SIMILI

Per i supporti magnetici e devices esterni si applicano gli stessi criteri che per i documenti cartacei e pertanto la loro custodia dovrà avvenire sempre sottochiave e non dovranno mai essere lasciati incustoditi. Tutti i file di provenienza incerta o esterna -ancorché attinenti all'attività lavorativa- devono essere sottoposti a controllo antivirus prima di essere aperti e/o utilizzati.

I supporti rimovibili (CD e DVD anche riscrivibili, supporti USB, hard disk ecc.) devono essere limitati a quelli strettamente indispensabili alle attività aziendali; in tali supporti non devono essere conservati, nemmeno provvisoriamente, file aziendali congiuntamente a file personali.

Non è permesso scaricare o copiare file contenuti in supporti removibili esterni (USB, hard disk drive, "chiavette USB", ecc..) se non attinenti alla propria attività lavorativa.

Nel caso in cui dati, informazioni, immagini e/o notizie aziendali e/o dati riservati devono essere salvate su supporti removibili, è obbligatorio conservare, custodire e controllare tali supporti affinché nessun soggetto terzo non autorizzato ne prenda visione o possesso. L'utente assegnatario è l'unico responsabile della custodia dei supporti e dei dati in essi contenuti. I supporti rimovibili devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato e/o alterato e/o distrutto, o, successivamente alla cancellazione, recuperato. Al fine di assicurare la distruzione e/o inutilizzabilità di supporti rimovibili, ciascun utente dovrà utilizzare gli strumenti messi a disposizione dal sistema operativo in uso per procedere alla formattazione a basso livello del supporto.

L'amministratore di sistema ha in ogni caso la possibilità di impedire ad ogni singola macchina e/o utente l'utilizzo di suddetti supporti.

UNITÀ DI RETE, MEMORIZZAZIONE FILE E BACKUP

Il disco fisso locale (quindi le cartelle di utilizzo frequente come Desktop, Documenti, etc..) del proprio PC deve essere utilizzato per la sola memorizzazione di file di interesse aziendale. La memorizzazione deve essere limitata a poche ore lavorative dal momento che questi dischi non sono sottoposti a backup. Tutti i file di rilevanza aziendale devono essere salvati sulle aree comuni o sulle aree personale delle share di rete (cartella My Home). È assolutamente da evitare la conservazione in rete di file obsoleti e/o inutili e/o ridondanti e per questo si invita il dipendente ad un attento ed ordinato utilizzo dello spazio di rete.

Qualsiasi file estraneo all'attività lavorativa e/o non espressamente autorizzato, non può, nemmeno in via transitoria, essere salvato sul PC in uso del dipendente e tanto meno essere salvato sulla rete aziendale. La competenza e la gestione delle aree di interesse comune è demandata ai responsabili di funzione di ciascuna area che provvederà ad indicare ai propri collaboratori i criteri sulle modalità di salvataggio e protocollo dei documenti.

Casa di Cura Villa Esther per mezzo dei sui fornitori gestisce lo storage aziendale; i dati conservati in tali aree sono protetti da procedure di backup automatico gestite e monitorate dal concessionario stesso; la policy attuale è configurata per un backup giornaliero e un'archiviazione full mensile con profondità di 1. Il backup incrementale salva i dati inseriti o modificati rispetto all'ultimo backup incrementale eseguito; qualora un file venisse cancellato, può essere ripristinato dai salvataggi per 7 giorni (per poi essere rimosso). Ogni mese viene fatta un'archiviazione completa dei dati, una sorta di fotografia dei dati presenti in quel momento. Questo salvataggio viene mantenuto nei backup per 1 anno. Alla fine dell'anno il salvataggio viene cancellato. Per il ripristino dei dati accidentalmente persi o modificati sulle cartelle di rete è fatto obbligo di avvisare tempestivamente la struttura I.T.

Le copie di backup sono memorizzate di norma su supporti/sistemi custoditi fisicamente in locali ad accesso controllato in completa gestione mentre almeno una copia di backup di alcuni tipi di dati più importanti viene memorizzata su supporti/sistemi distinti logicamente o fisicamente e non direttamente accessibili al sistema stesso.

Le cartelle di rete presenti negli storage sono aree di condivisione di informazioni strettamente professionali e non devono in alcun modo essere utilizzate per scopi diversi; qualunque file non legato all'attività lavorativa non può essere dislocato, nemmeno temporaneamente, in queste unità. Il personale della struttura I.T., senza necessità di esplicita autorizzazione, si riserva la facoltà di procedere alla verifica ed eventuale rimozione di qualsiasi file memorizzato nelle cartelle di rete qualora ritenuto pericoloso per la sicurezza o non attinente all'attività lavorativa. I privilegi di lettura e scrittura delle cartelle vengono definiti dal responsabile di struttura (o suo delegato) valutando il bilanciamento delle esigenze della produttività e della necessaria riservatezza. Tramite una stringente policy aziendale non è data all'utente la possibilità di modificare tali permessi.

Nel caso di cessazione del rapporto di lavoro (mobilità in uscita, pensionamento, dimissioni o decesso), trascorsi ulteriori 60 giorni, periodo stimato pertinente e non eccedente a garantire l'operatività e la continuità di servizio, salvo diverse indicazioni degli assegnatari o dei responsabili, specifiche richieste e casi particolari che verranno opportunamente trattati, il personale della struttura I.T. procederà alla cancellazione definitiva della cartella di rete assegnata in modalità esclusiva e non sarà possibile recuperare i dati in essa contenuti.

MOVIMENTAZIONE DI DATI CON PARTICOLARI REQUISITI DI RISERVATEZZA

Nell'invio di dati afferenti alle "categorie particolari" secondo il Regolamento UE 2016/679 tramite posta elettronica, la spedizione del file deve avvenire in forma di allegato e non come testo del messaggio. Il file allegato dovrà essere protetto con modalità idonee a impedire l'illecita o fortuita acquisizione da parte di soggetti diversi dal destinatario che potrà

consistere in una password per l'apertura del file o in una chiave crittografica rese note agli interessati attraverso separata comunicazione (come richiesto dalla vigente normativa).

UTILIZZO INTERNO ED ESTERNO DELLA POSTA ELETTRONICA ORDINARIA

L'indirizzo e-mail assegnato da Villa Esther ai dipendenti è uno strumento di lavoro di proprietà aziendale concesso in uso al lavoratore per un più proficuo svolgimento della prestazione. La Posta Elettronica può essere rilasciata "ad personam", associata ad un ufficio o ad una specifica funzione/progetto/servizio. Le persone assegnatarie delle caselle sono responsabili del corretto utilizzo delle stesse. Tale indirizzo va utilizzato in via esclusiva per tutta la corrispondenza elettronica in entrata ed in uscita. È espressamente vietato utilizzare caselle di posta diverse da quella assegnata reperibili in Internet, quali webmail fornite, ad esempio, da Yahoo, Libero, Hotmail, etc

La posta elettronica è controllata da una piattaforma Google Workspace.

Il dipendente è responsabile del contenuto dei messaggi inviati: al fine di garantire la sicurezza dei sistemi informativi aziendali è vietato utilizzare le caselle di posta assegnate per l'invio di messaggi personali o di contenuto extra lavorativo.

Non è consentito l'utilizzo di caselle di posta elettronica personali, al di fuori di quella aziendale, per le comunicazioni istituzionali. Non è altresì permesso l'utilizzo di caselle di posta aziendali diverse da quella/e assegnate. Tutte le mailbox sono configurate affinché eventuali comunicazioni email indirizzate al di fuori del dominio aziendale riportino un messaggio in calce nel quale viene dichiarata la natura non personale del messaggio nonché i vincoli in materia di riservatezza, con precisazione che le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente.

Gli allegati ai messaggi in entrata in formato non intrinsecamente sicuro vanno prima di qualsiasi altra iniziativa quando non ne sia personalmente noto il mittente. Gli allegati vanno se possibile trasmessi in formato universale e sicuro (PDF/A).

Tutti i messaggi e-mail da e per l'esterno sono di esclusiva disponibilità dell'Azienda, che potrà accedervi in qualsiasi momento, considerati i fini per cui tale utilizzo è ammesso ai sensi della presente policy. Non sono ammessi contenuti ed utilizzi diversi da quelli richiesti dalle finalità lavorative ed organizzative proprie dell'Azienda per il cui raggiungimento l'Azienda acconsente all'impiego di tale strumento.

SOCIAL NETWORK

Non è consentito l'utilizzo di alcun Social Network se non preventivamente autorizzato dalla Direzione Aziendale.

Il dipendente nell'utilizzo in forma privata, fuori dell'ambiente di lavoro, dei propri profili social è tenuto, anche in quanto pubblico dipendente, a non effettuare commenti denigratori o lesivi in genere della dignità di terzi e/o dell'Azienda. È altresì fatto assoluto divieto pubblicare qualsiasi contributo in forma di immagine o altro formato che possa essere lesivo della dignità, reputazione di terzi e/o dell'Azienda.

Quale conseguenza di utilizzo improprio dei propri profili social potranno essere attivati dall'Azienda procedimenti disciplinari a carico del responsabile e richieste di risarcimento dei danni eventualmente subiti da Villa Esther.

L'Azienda, qualora approvasse l'utilizzo di Social all'interno dell'amministrazione, si riserva la facoltà di attivare profili ufficiali aziendali strettamente correlati all'attività lavorativa.

UTILIZZO DELLA RETE FISICA LOCALE (LAN)

Tutte le postazioni di lavoro operano interconnesse alla rete aziendale e possono così accedere ai dati secondo precise abilitazioni. La rete aziendale interna non può esser utilizzata per scopi diversi da quelli ai quali è destinata.

La configurazione e la gestione di tutti gli apparati attivi e dell'infrastruttura di collegamento sono affidati al settore I.T.

Non è consentita la connessione alla rete aziendale di apparati atti ad effettuare connessioni con altre reti verso l'esterno (router, bridge, modem, impianti wireless, ecc.). Un eventuale uso di tali apparati, qualora necessario, dovrà essere richiesto alla struttura I.T. e ricevere autorizzazione dalle Direzioni competenti. Analogamente non è ammesso, se non per esigenze estemporanee e previa autorizzazione della struttura I.T., l'utilizzo non autorizzato di dispositivi per lo sdoppiamento di punti rete (mini Hub/switch).

Viene fatto esplicito e tassativo divieto di connettere in rete stazioni di lavoro ed ogni altro dispositivo informatico (es. computer e portatili non aziendali) se non previa esplicita e formale autorizzazione della struttura I.T.

È fatto assoluto divieto di configurare servizi già messi a disposizione in modo centralizzato, quali ad esempio, e non solo, DNS, DHCP, NTP, mailing, accesso remoto, proxy server.

È fatto assoluto divieto all'utente di intercettare ed analizzare i pacchetti sulla rete aziendale, utilizzando analizzatori di rete sia software che hardware. Nel caso si riscontrasse la presenza di PC che generano traffico anomalo o che potrebbero far diminuire le prestazioni dell'intero sistema, sarà facoltà del personale della struttura I.T. procedere al blocco, se necessario, dell'attività di rete della postazione.

È fatto divieto di svolgere attività intenzionali che portino in qualunque modo alla saturazione dei sistemi di elaborazione e di trasmissione dati, rendendo anche temporaneamente indisponibili risorse di uso comune agli utenti.

Non è consentito l'accesso agli armadi di rete, la modifica delle connessioni o la manomissione di qualunque impianto o cavo vi sia contenuto.

UTILIZZO DELLA RETE WIRELESS (WLAN)

Ad integrazione della rete LAN descritta nella precedente, alcune aree della Casa di Cura Villa Esther sono servite da reti non cablate -Wireless LAN- per consentire la trasmissione dei dati attraverso canali senza fili. Utilizzando specifici apparati Access Point vengono distribuiti tre SSID: “Villa Esther Admin”, “Villa Esther System”, “Villa Esther Ospiti”.

La WiFi-LAN “Villa Esther System” risulta a tutti gli effetti un’estensione della rete LAN, pertanto, i client connessi, avranno la possibilità di accedere alle medesime risorse della rete locale cablata. La tecnologia è configurata e governata e solo l’amministrazione dispone per il rilascio delle abilitazioni per il tramite della struttura I.T. su comunicazione del MAC-ADDRESS dell’appartato. È fatto divieto assoluto di connettersi a tale infrastruttura utilizzando sistemi diversi dai dispositivi aziendali quali portatili e tablet preventivamente configurati dalla struttura I.T. (per esempio, è vietata la connessione di cellulari, oppure laptop e tablet personali).

La rete “Villa Esther System” è utilizzata al solo scopo di interconnessione dei sistemi strettamente legati al funzionamento delle periferiche di sistema. È tecnologicamente inibita qualunque connessione non preventivamente accordata dal servizio I.T.

La rete “Villa Esther Ospiti” è una rete wireless per fornire connettività Internet agli ospiti della struttura con la possibilità di collegare temporaneamente i propri dispositivi. La rete è completamente scollegata a livello logico da tutta l’infrastruttura informatica dell’azienda e l’accesso è consentito tramite l’utilizzo di credenziali di accesso fornite dall’accoglienza della struttura. L’utilizzo del servizio è regolato da una direttiva interna.

INTERNET

Il PC abilitato alla navigazione in Internet costituisce uno strumento necessario allo svolgimento della propria attività lavorativa. È pertanto vietato accedere a siti il cui contenuto non è riconducibile all’attività lavorativa. L’abilitazione alla navigazione è assegnata a livello di utenza e deve essere autorizzata dal responsabile di struttura (o suo delegato) che invia opportuna richiesta alla struttura I.T.

È attivo un sistema di protezione della navigazione Internet che prevede il filtraggio automatico del traffico per categorie di contenuti ed è inoltre presente la funzionalità di gestione di specifiche blacklist di url.

È vietata la connessione alla rete Internet mediante l'autonoma installazione di modem, router o altri apparecchi di connettività.

Non è consentito scaricare o copiare (download/upload) di file o software di ogni genere da siti internet accedendo abusivamente ad un sistema informatico o telematico protetto da misure di sicurezza. Allo stesso modo non è consentita la permanenza in un sistema informatico o telematico, servizio applicativo in genere contro la volontà espressa o tacita dell'Azienda.

La Casa di Cura Villa Esther si cautela nei confronti di tali attività bloccando l'accesso a siti Internet non pertinenti l'attività lavorativa e comunque tracciando tutte le attività di navigazione effettuate all'interno dell'azienda stessa.

Ogni file (o software) eventualmente scaricato da Internet avviene sotto la responsabilità esclusiva di ciascun dipendente e deve essere necessariamente preceduto da una analisi volta a verificare l'eventuale presenza di virus; ciò a tutela dell'integrità del patrimonio aziendale. Qualora il singolo utilizzatore dipendente non sia in grado di procedere autonomamente e correttamente al predetto controllo, dovrà contattare la struttura I.T., prima di procedere a qualsiasi operazione che comporti il prelevamento di file da siti Internet.

Non è consentito l'utilizzo dei servizi di messaggistica istantanea -esclusi quelli espressamente autorizzati dall'azienda- programmi di condivisione file (file sharing) e di programmi P2P.

È rigorosamente vietata la registrazione e partecipazione a forum non professionali, l'utilizzo di chatline, di social network, di bacheche elettroniche (esclusi quelli espressamente autorizzati dall'azienda) le registrazioni in guest books anche utilizzando pseudonimi.

Non è consentita alcuna attività legata ad operazioni di hackeraggio e pirateria informatica in generale. È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo i casi direttamente autorizzati dai Responsabili e con il rispetto delle normali procedure d'acquisto.

INSTALLAZIONE SOFTWARE

L'installazione di software deve avvenire esclusivamente ad opera di soggetti provvisti di specifiche abilitazioni preventivamente autorizzati dalla struttura I.T. I software e gli applicativi installati sono parte del patrimonio aziendale e come tali devono essere utilizzati nel rispetto della presente policy e di eventuali indicazioni ricevute dalla struttura I.T.

Al fine di tutelare il sistema informatico -sussistendo il grave pericolo di introdurre codice malevolo e/o di alterare la funzionalità delle applicazioni software esistenti- è fatto divieto a chiunque utilizzi computer aziendali di scaricare dalla rete Internet (installare e/o eseguire) qualsiasi tipo di software non autorizzato.

Non è consentito l'utilizzo di software che consenta l'accesso alla postazione di lavoro - controllo remoto - o ai dati istituzionali al di fuori della rete aziendale (condivisione dati online), ad esclusione degli eventuali applicativi preventivamente forniti ed autorizzati dalla struttura I.T.

Al fine di tutelare l'integrità e la veridicità dei documenti informatici, è vietata la installazione e l'utilizzo di software (e hardware) atti ad intercettare, falsificare, alterare, impedire e interrompere comunicazioni (e/o il contenuto documenti informatici); è altresì vietata l'installazione di software che potrebbero rivelarsi lesivi del sistema informatico aziendale.

Non è permesso l'utilizzo di programmi diversi da quelli ufficialmente installati dalla struttura I.T. Al fine di proteggere l'integrità dell'Azienda, il personale non può utilizzare software di proprietà personale, comprese applicazioni regolarmente acquistate e registrate, programmi shareware e/o freeware, eventuale software scaricato da Internet o proveniente da CD/DVD allegati a riviste e/o giornali o altro software posseduto a qualsiasi titolo.

Non è consentita l'installazione, anche se necessaria, di eventuali driver per stampanti o altri supporti (come ad esempio masterizzatori, scanner, etc.); in questo caso l'utente dovrà richiedere ai tecnici della struttura I.T. di intervenire per effettuare l'installazione.

L'installazione volontaria sul personal computer in dotazione di componenti software in grado di danneggiare, deteriorare o rendere, in tutto o in parte, inservibile il sistema informatico o le informazioni in esso contenute, può costituire, tenuto conto della gravità del comportamento, condotta sanzionata penalmente ai sensi dell'art. 635-bis Cod. Pen.

Sono in uso particolari software volti a fornire, con cadenza programmata (attualmente, la pianificazione è settimanale) report specifici in merito ai software installati nelle postazioni di lavoro. Su tali report sono effettuate attività di analisi volte a rilevare la presenza di software non autorizzato. Gli aggiornamenti del sistema operativo sono necessari, oltre che per obbligo di legge, al fine di proteggere i PC e l'intera rete. È stato attivato il Windows Server Update Services (WSUS) che pianifica e dispone l'installazione degli aggiornamenti in modalità automatica.

È tassativamente vietato all'utente ogni sorta di aggiornamento manuale del software installato se non espressamente autorizzato dalla struttura I.T. Gli aggiornamenti del software e dei driver necessari al buon funzionamento della postazione di lavoro saranno effettuati direttamente dai tecnici della struttura I.T. configurando gli aggiornamenti automatici per ciò che attiene la protezione antivirus ed il sistema operativo, ed intervenendo dietro segnalazione dell'utente per ogni ulteriore update si dovesse rendere necessario.

ANTIMALWARE

Villa Esther utilizza il servizio Antivirus erogato da Microsoft e insito nel sistema operativo. La politica di sicurezza aziendale prevede l'installazione di un software anti malware (antivirus) su tutte le postazioni di lavoro (che lo supportano); esso viene aggiornato automaticamente grazie ad una gestione centralizzata per mezzo di un server dedicato. Sulle postazioni eventualmente off-line, tali aggiornamenti vengono installati non appena si ripresenteranno in linea, di norma, alla prima accensione. Tale modalità permette di elevare al massimo la protezione contro virus ed agenti esterni.

Non è ammesso l'utilizzo di sistemi antivirus diversi, se non espressamente autorizzato dalla struttura I.T.

È stata inoltre abilitata di default su tutti i client la modalità "Scan all files in removable storage devices after plugin" atta ad effettuare la scansione di tutte le periferiche rimovibili che vengono collegate. È inoltre attivo il blocco dell'esecuzione "autorun" che disinnesca l'esecuzione automatica di contenuti al momento della connessione dei dispositivi mobili.

Nel caso il software antivirus rilevi la presenza di un virus che non è riuscito a ripulire, l'utente dovrà immediatamente:

- sospendere ogni elaborazione in corso senza spegnere il computer;
- segnalare l'accaduto all'HelpDesk preposto secondo le vigenti disposizioni.

APPARECCHIATURE DI RIPRODUZIONE/REGISTRAZIONE IMMAGINI

È vietata l'esecuzione di riproduzione/registrazione di immagini, a qualsiasi titolo, con apparecchiature personali o di terzi, se non espressamente autorizzati dalla Direzione Aziendale.

Non è consentito l'utilizzo di sistemi di videoconferenza/audioconferenza se non preventivamente autorizzati dalla struttura I.T. - sussistendo il grave pericolo di introdurre codice malevolo e/o di alterare la funzionalità delle applicazioni software esistenti.

PIANO CONTINUITÀ OPERATIVA

PREMESSA

La Casa di Cura Villa Esther ha adottato il seguente Piano di Continuità Operativa documentato (BCP) integrandolo con una politica di Disaster Recovery (DR) che definisce i possibili disastri e gli scenari di rischio, individua i processi critici e le figure di riferimento, interne ed esterne alla Società, in caso di gravi problemi oltre che le modalità di risoluzione degli stessi.

RUOLI E RESPONSABILITÀ NEL RIPRISTINO DELLE INFORMAZIONI

La Casa di Cura Villa Esther….

POSSIBILI SCENARI DI CRISI E CLASSIFICAZIONE DEGLI INCIDENTI

La Casa di Cura Villa Esther….

VALUTAZIONE DEI SERVZI ESSENZIALI DA RIPRISTINARE E TEMPISTICHE

La Casa di Cura Villa Esther….

PROCEDURA DI RECUPERO DATI

La Casa di Cura Villa Esther….