REGIONE DEL VENETO

ULSS5 POLESANA

DISCIPLINARE PER L'UTILIZZO DEI SISTEMI INFORMATICI E DI ALTRI DISPOSITIVI ELETTRONICI

Sommario

PREMESSA

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer, espone l'Amministrazione non soltanto a rischi di natura patrimoniale, ma anche alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge, creando problemi alla sicurezza ed all'immagine dell'Ente stesso.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche dell'Ente deve sempre ispirarsi al principio di diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto contrattuale, dipendente o meno, sono state redatte in questo documento delle indicazioni nell'uso delle apparecchiature informatiche al fine di evitare che comportamenti non idonei possano innescare problemi o minacce alla Sicurezza.

1. INDICAZIONI PER L'UTILIZZO DEL PERSONAL COMPUTER

Il Personal Computer utilizzato dall'utente è uno strumento di lavoro che deve essere custodito con cura evitando il più possibile ogni forma di danneggiamento ed utilizzo al di fuori dell'attività lavorativa.

L'accesso ad ogni personal computer è protetto da password che deve essere custodita dall'utente con la massima diligenza e non divulgata.

Sono vietati l'uso e/o l'installazione di programmi diversi da quelli distribuiti ed installati ufficialmente dall'UOS Sistemi Informativi dell' AZIENDA come previsto dalla normativa AGID (ABSC 2.3.1). L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'Ente a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (D. Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore. Nel caso fossero necessari ulteriori programmi, gli stessi dovranno essere autorizzati dalla Direzione Aziendale.

Il Personal Computer deve essere spento prima di lasciare gli uffici o nel caso di assenza prolungata; nel caso di breve e temporaneo inutilizzo, ad esempio nella pausa pranzo, la postazione deve essere bloccata tramite la combinazione dei tasti WINDOWS + L, o in alternativa deve essere fatta la disconnessione del proprio utente in maniera tale da impedirne l'utilizzo a

personale non autorizzato.

Lo spegnimento e successiva riaccensione del P.C. almeno una volta al giorno consente l'applicazione degli aggiornamenti atti a correggere le vulnerabilità del sistema come previsto dalla normativa AGID (ABSC 4.5.1).

Si ricorda inoltre che tutti i dischi e altre unità di memorizzazione locali (es. Disco C, chiavette, dischi esterni) non sono soggette a salvataggio da parte dell'UOS Sistemi Informativi.

1.1. Interventi di sicurezza e salvaguardia

Il personale incaricato che opera presso la UOS Sistemi Informativi è stato autorizzato a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.). La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Azienda, si applica anche in caso di assenza prolungata o impedimento dell'utente. Qualora lo specifico intervento dovesse comportare anche l'accesso a contenuti delle singole postazioni PC, il responsabile del dipendente/utente interessato ne darà comunicazione allo stesso, preventivamente ovvero, nel caso di urgenza dell'intervento stesso, successivamente ad esso. Detti interventi dovranno essere richiesti dalla Direzione Aziendale o dal Dirigente responsabile del servizio/ufficio alla UOS Sistemi Informativi a mezzo di richiesta formale tramite mail o protocollo.

2. INDICAZIONI PER L'UTILIZZO DI DOTAZIONI INFORMATICHE PORTATILI

L'utente è responsabile delle dotazioni informatiche portatili, quali notebook, tablet, smartphone, ecc… assegnategli e deve custodirle con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Alle dotazioni informatiche portatili si applicano le regole di utilizzo previste per i P.C. connessi in rete, eventuali regole particolari di utilizzo saranno concordate direttamente con il responsabile dell'UOS Sistemi Informativi e gli utenti interessati.

Deve essere posta massima attenzione alla custodia delle dotazioni informatiche portatili durante il loro utilizzo ed in particolare all'esterno delle sedi istituzionali dell'Ente.

3. UTILIZZO DI FOTOCOPIATRICI E STAMPANTI LOCALI E DI RETE

È cura degli utenti effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti (soprattutto per le stampanti di rete site in luoghi facilmente accessibili al pubblico), al fine di evitare che possano essere visionate da persone non autorizzate.

È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati) su stampanti comuni.

È inoltre sconsigliato la stampa di email, ricevute di posta elettronica certificata e altri documenti che sono facilmente reperibili dalle risorse informatiche a disposizione.

Si consiglia sempre di effettuare l'anteprima di stampa prima della stampa effettiva, al fine di verificare la correttezza della stampa ed evitare di mandare in stampa documenti non impostati correttamente.

Nel momento in cui si inserisce la carta nei cassetti di alimentazione, evitare di inserire carta sgualcita, rovinata o umida.

Quando si cambiano le impostazioni di un fotocopiatore e/o stampante, alla fine del proprio lavoro, si deve in seguito ripristinare l'assetto originario.

Quando si finisce la carta nei fotocopiatori di rete, è buona norma ricaricare la macchina, in modo che i successivi fruitori la trovino pronta per l'utilizzo.

Si consiglia di prestare attenzione al destinatario nel momento di inoltro di scansione da fotocopiatore di rete a mail aziendale, al fine di evitare l'invio a persone non autorizzate a leggere quanto contenuto dalla stessa.

4. UTILIZZO DELLE CARTELLE DI RETE

Le cartelle di rete (cartelle dedicate ai servizi presenti sul server) sono aree di condivisione di informazioni strettamente professionali e non possono essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere memorizzato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup, da parte dell'UOS Sistemi Informativi.

Nel caso in cui vengano rilevati dei file impropriamente memorizzati nelle cartelle di rete, questi verranno eliminati d'ufficio.

Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati: è infatti da evitare un'archiviazione ridondante che comporta inutili costi aggiuntivi.

Si consiglia inoltre di utilizzare nomi di file e cartelle brevi e di non creare troppe cartelle nidificate, in quanto, potrebbero presentarsi problemi di ripristino nel caso di eventuale necessità di recupero dei file/cartelle dal backup.

5. INDICAZIONI PER L' UTILIZZO DEI SUPPORTI REMOVIBILI

È fatto assoluto divieto di memorizzare i dati sensibili nei supporti removibili (penne USB, HD esterni USB, CD, DVD) che devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato, divulgato, alterato e/o distrutto o successivamente alla cancellazione, recuperato.

Nel caso in cui i dati sensibili siano memorizzati nei supporti removibili, ai fini di creare dei salvataggi, questi devono essere custoditi in archivi chiusi a chiave. L'utente è responsabile della custodia dei supporti e dei dati in essi contenuti.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente la UOS Sistemi Informativi nel caso in cui vengano rilevati virus o altri comportamenti informatici anomali.

Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali come previsto nella normativa AGID (ABSC 8.3.1).

6. ANTIVIRUS

Il sistema informatico dell'Azienda è protetto da software antivirus centralizzato, n ella modalità Client/Server, aggiornato periodicamente.

Nel caso in cui il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso e segnalare prontamente l'accaduto al servizio di assistenza dell'UOS Sistemi Informativi.

I Virus di tipo "ransomware" continuano a rappresentare la minaccia più temuta. In questo tipo di minaccia i criminali informatici puntano a sfruttare i punti deboli umani, i cattivi comportamenti e la scarsa attenzione che la maggioranza degli utenti ripone nell'utilizzo degli strumenti informatici.

Il ransomware ("ransom" significa riscatto) è una forma di malware che impedisce all'utente di accedere ad aree del proprio computer perchè crittografa i files o protegge l'hard disk dagli accessi, visualizzando un messaggio che forza l'utente a pagare per riavere accesso al computer.

Questo tipo di malware si diffonde attraverso file scaricati o vulnerabilità presenti nei P.C. non aggiornati e nei servizi di rete.

È bene quindi verificare che l'antivirus sia installato ed aggiornato come previsto dalla normativa AGID (ABSC 8.1.1). Per fare cio occorre tramite il puntatore del mouse posizionarlo

sull'Area di notifica, situata in basso a destra del Desktop, sopra l'icona del simbolo dell'antivirus, cliccare con il tasto destro del mouse, ed scegliere l'opzione '*Apri console*'.

Verrà visualizzata la data e ora dell'ultimo aggiornamento effettuato che nel caso corrispondesse al giorno precedente si deve fare immediatamente l'aggiornamento. L'azienda per quanto possibile imposterà delle politiche di configurazione in modo da:

a) evitare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili. AGID (ABSC 8.7.1)
b) evitare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file. AGID (ABSC 8.7.2)
c) evitare l'apertura automatica dei messaggi di posta elettronica. AGID (ABSC 8.7.3)
d) evitare l'anteprima automatica dei contenuti dei file. AGID (ABSC 8.7.4).

Ogni utente deve comunque tenere comportamenti rispettosi di quanto appena descritto in modo da ridurre il rischio di attacco al sistema informatico dell'Ente da parte di virus o altro software dannoso.

7. GESTIONE DELLE PASSWORD

Le credenziali di autenticazione per l'accesso al computer, alla mail ed ai software applicativi vengono assegnate dal personale dell'UOS Sistemi Informativi, previa ricezione del modulo di richiesta appositamente predisposto, debitamente compilato dal Direttore/Responsabile della UOC/UOS di appartenenza ed autorizzato dalla DMPO o dalla Direzione di riferimento.

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (userid) associato ad una parola chiave (password) riservata che dovrà essere modificata al primo accesso e custodita dall'utente con la massima diligenza e non divulgata. È proibito entrare nei P.C. e nei programmi con credenzali non proprie.

La password è la prima protezione ai dati, non deve essere ceduta ad altri, non deve essere scritta in un foglietto lasciato sullo schermo o sulla scrivania. Ciascun utente è responsabile delle proprie credenziali per cui, se dovessero essere usate da altri in modo improprio, la colpa ricadrebbe sull'utente stesso.

È buona regola impostare la password:

- con una sequenza minima di 8 caratteri alfanumerici
- utilizzando caratteri maiuscoli, minuscoli, numeri
- utilizzando caratteri speciali, come @ # $ % ^ &
- alternando maiuscole a minuscole.

Nel creare una password sicura è altresì buona norma non usare parole comuni per la password così che non sia riconducibile all'incaricato, come ad esempio:

- la data di compleanno
- il proprio nome utente (User-ID).

Al fine di aumentare il grado di sicurezza è consigliabile creare password diverse per tipologie diverse di utilizzo, quindi è buona norma utilizzare password diverse per gli account private e quelli aziendali. Questo al fine di evitare che, se la propria password venisse scoperta da un malintenzionato, questo possa accedere a tutti i servizi.

Il sistema di autenticazione del dominio/posta interno provvede 5 giorni prima della scadenza, a richiedere la variazione della password agli utenti, si invitano pertanto gli utenti ad effettuare il cambio password prima della sua scadenza. Per le altre autenticazioni, ove non sono previsti sistemi automatizzati di rinnovo delle password, si invitano gli utenti, prima della scadenza, a variare la propria password periodicamente attraverso i sistemi delle singole applicazioni.

8. UTILIZZO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

La navigazione in Internet costituisce uno strumento necessario allo svolgimento della propria attività lavorativa.

Per ragioni di sicurezza è stato implementato un servizio di filtro dei siti internet, che permette di inibire o limitare l'accesso a siti i cui contenuti siano classificati pericolosi o non attinenti agli scopi istituzionali, sono pertanto da evitare tutte le azioni atte ad eludere tali politiche di filtro.

Si informa che l'UOS Sistemi Informativi dispone di strumenti di controllo che evidenziano le attività di elusione delle politiche di filtro.

È necessario evitare di collegare il telefonino al computer anche solo per la ricarica in quanto tale azione potrebbe essere considerata dai sistemi di controllo una elusione al filtro.

Qualora tali sistemi di filtro impediscano l'utilizzo di siti o risorse utili all'attività lavorativa, l'utente interessato dovrà richiedere lo sblocco alla UOS Sistemi Informativi, inoltrando richiesta scritta e motivata, controfirmata dal responsabile della propria Unità/Area.

È facoltà dell'UOS Sistemi Informativi inibire temporaneamente, anche senza preavviso, la navigazione in internet alle postazioni dove si prefiguri un utilizzo improprio o che metta a repentaglio la sicurezza del Sistema informatico dell'Ente.

È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa, compresa la partecipazione a forum non professionali.

9. UTILIZZO DELLA POSTA ELETTRONICA

La casella di posta istituzionale, assegnata dall'Amministrazione all'utente, è uno strumento

di lavoro consentito per finalità connesse allo svolgimento della propria attività lavorativa. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

La casella di posta deve essere mantenuta in ordine, controllando periodicamente il rispetto della dimensione assegnata, mantenendo pulita la cartella "Cestino" / "Posta Eliminata".

Per la trasmissione di files è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati; per gli scambi di files tra colleghi si incoraggia l'utilizzo delle cartelle condivise esistenti.

Per la casella di posta elettronica su Gmail è stata implementata l'autenticazione a più fattori. Questo è un metodo di autenticazione elettronica in cui a un utente viene concesso l'accesso solo dopo aver presentato con successo due o più prove a un meccanismo di autenticazione. L'autenticazione a più fattori innalza il livello di sicurezza informatica proteggendo i danni provocati da furti di password da parte di malintenzionati.

9.1 Norme di comportamento sull'utilizzo delle e-mail aziendali

1) LA CASELLA DI POSTA ELETTRONICA È UNO STRUMENTO DI LAVORO

Le persone assegnatarie di una casella di posta elettronica sono responsabili del corretto utilizzo delle stesse. L'utilizzo delle e-mail deve essere limitato esclusivamente per scopi lavorativi. L'eventuale personalizzazione degli indirizzi e-mail assegnati non implica o giustifica per quegli stessi indirizzi e-mail un carattere privato, in quanto trattasi di strumenti di esclusiva proprietà aziendale, messi a disposizione del dipendente al solo fine dello svolgimento delle proprie mansioni lavorative.

2) UTILIZZARE UN OGGETTO BREVE E CONCISO

L'oggetto è ciò che convince i destinatari ad aprire o meno l'e-mail. Nelle prime righe della **e-mail** in genere dovrebbero essere racchiuse tutte le informazioni essenziali che si intende comunicare.

Tra le comunicazioni che si ricevono quotidianamente, infatti, è importante consentire al proprio interlocutore di percepire l'importanza di aprire l'e-mail e leggere il resto.

3) USARE FORME DI SALUTO PROFESSIONALI

Anche se si ha un rapporto confidenziale con il proprio interlocutore, in una e-mail è bene trovare l'equilibrio tra un'eccessiva formalità e il tono amichevole, usando sempre un registro adeguato e rispettoso nei confronti del destinatario, ricordando che il mittente è sempre un utente di Azienda ULSS 5 Polesana, e in quanto tale, referente di una pubblica istituzione.

4) INTERPRETARE L'USO DEL CAPS LOCK (tasto fissa maiuscole) E DELLA PUNTEGGIATURA

Anche se potrebbe sembrare banale, scrivere in maiuscolo e concludere la frase con più di un punto esclamativo darà un'idea di scarsa maturità professionale a chi riceve l'e-mail, apparendo decisamente eccessivo. Va ricordato che in Rete il maiuscolo viene utilizzato come l'equivalente di un urlo o comunque di una parola pronunciata ad alta voce. È possibile ricorrere a sigle ed acronimi, purché già sdoganati e non di nostra invenzione. È possibile ricorrere alle emoticon (le cosiddette "faccine") da usare, però, con moderazione e solo se il contesto del messaggio lo richiede.

5) L'IMPORTANZA DI RISPONDERE IN TEMPI BREVI

Per quanto possa risultare difficile rispondere repentinamente a tutte le e-mail ricevute, bisognerebbe provare a farlo: la comunicazione informatica ha la stessa importanza di una telefonata o di un incontro di persona. Secondo le regole di netiquette, **è buona educazione rispondere anche alle e-mail ricevute per errore, informando il mittente del disguido,** e provvedendo alla successiva eliminazione, in quanto non autorizzati al trattamento dei dati comunicati con l'errato invio**.**

6) PRIMA RILEGGERE, POI INVIARE

E-mail con errori grammaticali difficilmente passano inosservate al destinatario. Percepirà una scarsa attenzione e cura: **rileggere più volte il messaggio prima di inviarlo aiuta a mantenere sempre alto il livello di professionalità e accuratezza.**

7) PRIMA IL CORPO DEL MESSAGGIO, POI GLI ALLEGATI, ALLA FINE I DESTINATARI

Anche ai più attenti e scrupolosi può capitare di cliccare accidentalmente il tasto "invio", prima di aver terminato la scrittura, o non aver ancora messo gli allegati.

La scelta dei destinatari quindi deve essere oculata, rispettare eventuali gerarchie presenti in azienda ed essere selettiva: per esempio, evitare di inserire in copia conoscenza utenti non indispensabili o non interessati al contenuto della **e-mail**. Anche nel momento in cui si sta rispondendo ad una e-mail ricevuta, è opportuno **fare attenzione ad i destinatari**, controllando la correttezza degli indirizzi inseriti.

8) UTILIZZARE IL CAMPO CCN

Qualora la comunicazione debba essere inviata a più soggetti il cui indirizzo e-mail non appartiene all'organizzazione aziendale (@aulss5.veneto.it), è necessario provvedere ad un invio separato per ciascun destinatario, oppure inserendo questi stessi indirizzi **nel campo "CCN"** (*copia conoscenza nascosta o copia carbone nascosta*), così che non vi sia l'indebita o l'impropria condivisione di indirizzi e-mail tra tutti i destinatari.

9) PRESTARE ATTENZIONE AGLI ALLEGATI

Al messaggio di posta elettronica può essere aggiunto un **allegato**, testuale o multimediale. Citarlo nella e-mail può essere utile. Prima di inserire e inviare l'allegato è importante controllarne dicitura, estensione e dimensioni, per evitare che un file troppo "pesante" non arrivi a destinazione o impedisca l'invio della e-mail. È necessario controllare i file allegati di posta elettronica prima del loro utilizzo. In particolare, si deve evitare l'apertura e la lettura di messaggi di posta elettronica in arrivo provenienti da mittenti di cui non si conosce con certezza l'identità o che contengano allegati con estensione .exe, .com, .vbs, .htm, .bat, ecc.

Nessun documento contenente dati sanitari può essere condiviso tramite e-mail, se non applicando specifiche regole che garantiscano la riservatezza della comunicazione.

Qualora il titolare del trattamento intenda inviare copia del referto alla casella di posta elettronica dell'interessato, a seguito di sua richiesta, per il referto prodotto in formato digitale dovranno essere osservate le seguenti cautele:

a) spedizione del **referto in forma di allegato** a un messaggio e-mail e non come testo compreso nel corpo del messaggio;
b) il file contenente il **referto** dovrà essere **protetto** con modalità idonee a impedire l'illecita o fortuita acquisizione delle informazioni trasmesse da parte di soggetti diversi da quello cui sono destinati, che potranno consistere in una **password** per l'apertura del file **o** in una **chiave crittografica** rese note agli interessati tramite canali di comunicazione differenti da quelli utilizzati per la spedizione dei referti;
c) **convalida degli indirizzi e-mail tramite** apposita procedura di verifica on-line, in modo da evitare la spedizione di documenti elettronici, pur protetti con tecniche di cifratura, verso soggetti diversi dall'utente richiedente il servizio.

10) VALUTARE SE È MEGLIO PARLARNE DI PERSONA

Ci sono questioni particolarmente complesse per cui la posta elettronica andrebbe evitata, preferendo comunicazioni più dirette, come una telefonata o un incontro di persona, laddove possibile. Le e-mail molto lunghe e complicate possono essere fraintese, male interpretate o non del tutto comprese, ecco perché è meglio prediligere forme di comunicazione più immediate.

11) RICORDARE DI COMUNICARE LA PROPRIA IDENTITÀ

La firma del proprio messaggio dovrebbe fornire al destinatario, anche nel caso di un destinatario interno all'Azienda, le seguenti informazioni:

- Nome completo
- Ruolo all'interno dell'azienda
- Indirizzo
- Numero di telefono

Questi dati sono particolarmente importanti quando non c'è ancora stato alcun contatto al di là della comunicazione via e-mail. In questo modo il destinatario può all'occorrenza utilizzare forme di contatto alternative.

12) GESTIONE DELLA CASELLA DI POSTA ELETTRONICA

L'intestatario della casella di posta elettronica è tenuto alla gestione della propria casella. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati di dimensione elevata (previa archiviazione nella metodologia che si ritiene più adeguata se considerati di utilità per il proprio lavoro), al fine di evitare di esaurire lo spazio assegnato alla propria casella per la memorizzazione delle e-mail.

13) IMPOSTAZIONE DELLA E-MAIL DURANTE I PERIODI DI ASSENZA

Non è consentito l'invio automatico di e-mail all'indirizzo e-mail privato (attivando per esempio un "inoltro" automatico delle e-mail entranti), anche durante i periodi di assenza

programmata o non programmata (es. ferie, malattia, infortunio ecc.). In queste ipotesi, l'intestatario dell'indirizzo mail dovrà prevedere l'utilizzo di un messaggio "Fuori sede/Non in servizio", la cui attivazione/disattivazione è a suo carico, facendo menzione di chi, all'interno dell'Ente, sarà il proprio riferimento alternativo durante l'assenza. È bene, altresì, evitare l'invio di messaggi di posta elettronica in nome e per conto di un altro utente, salvo sua espressa autorizzazione. Nell'ipotesi di assenza, se l'intestatario è stato nell'impossibilità di inserire il messaggio nel risponditore automatico di posta elettronica, al fine di non pregiudicare la necessaria tempestività ed efficacia dell'intervento, il Dirigente responsabile inoltrerà specifica richiesta alla UOS Sistemi Informativi di accedere alla casella di posta del dipendente/utente al fine di inserire il messaggio automatico valevole per il periodo di tempo comunicato. Sarà carico dello stesso Dirigente informare il dipendente/utente di quanto attivato nelle impostazioni del suo indirizzo mail.

Le caselle di posta elettronica generiche o non nominative e le modalità di configurazione (e conseguentemente di accesso) possono essere di due tipi:

1. **Gruppo di distribuzione**: non richiede licenza aggiuntiva e quindi non ha costo. Le mail inviate a questo indirizzo vengono inoltrate a tutti i membri del gruppo, i quali, come requisiti, devono essere in possesso di mail Aziendale.

2. **Accesso in delega**: richiede una licenza aggiuntiva e obbligatoriamente tutti i delegati devono avere la mail Aziendale. L'accesso avviene direttamente da Gmail selezionando l'account appropriato. Tutti gli accessi sono tracciati.

In caso di cessazione del rapporto di lavoro o collaborazione o di mandato dei Direttori, la casella di posta elettronica individuale dell'interessato verrà sospesa per 30 giorni dalla data di cessazione del rapporto in essere. Trascorsi i 30 giorni la casella verrà eliminata.

Sarà cura dell'intestatario della casella di posta, prima della cessazione del rapporto in essere con l'Azienda, scaricare una copia dei messaggi e dei contatti presenti su GSuite.

La procedura da seguire è la seguente:

a) Entrare nella propria casella di posta
b) Dal pannello in alto a destra cliccare su Account e selezionare "Gestisci il tuo account Google"
c) Dalla videata che si apre selezionare Dati e personalizzazione
d) Scarica o Elimina i tuoi dati
e) Selezionare il servizio Posta e selezionare i dati per i quali si intende effettuare il backup
f) Selezionare eventualmente altri servizi per i quali si intende effettuare il backup
g) Procedere al passaggio successive

h) Impostare i parametri desiderati, tipicamente “Invia tramite e-mail il link per il download”
i) Premere crea archivio

Successivamente si riceverà via mail il link tramite il quale scaricare i file prodotti.

10. ISTRUZIONI PER PROTEGGERSI DAL PHISHING ED EVITARE LA SOTTRAZIONE DI DATI RISERVATI E PERSONALI AI SENSI DELL’ARTICOLO 32, COMMA 4, DEL REG (UE) 2016/679 (GDPR)

Il presente modulo intende fornire delle Istruzioni operative agli Incaricati, anche ai sensi dell’art. 32, comma 4 GDPR, in relazione al trattamento dei dati del Titolare effettuato per il tramite del servizio di posta elettronica, in considerazione del fatto che tale servizio, pur essendo protetto da strumenti che applicano politiche di antivirus ed antispam, potrebbe non bloccare email potenzialmente malevole.

Tali Istruzioni devono essere considerate quali direttive provenienti dal datore di lavoro il cui mancato rispetto potrebbe generare delle responsabilità a carico del dipendente.

10.1 Non utilizzare il proprio account e-mail fornito dal Titolare per usi personali

Il dipendente è tenuto a non utilizzare il proprio account e-mail fornito dall’Azienda per propri fini ed usi privati, quali, a titolo esemplificativo, scambi di e-mail con persone inerenti la propria sfera privata; partecipazione a gruppi di discussione; acquisti online su piattaforme di e-commerce (Amazon, Ebay e simili); ricezione di e-mail promozionali e pubblicitarie; iscrizione a siti non istituzionali o piattaforme di sociali network.

Ciò, infatti, comporta la circolazione e l’esposizione pericolosa dell’indirizzo istituzionale in ambiti dove operano malintenzionati. Un simile comportamento, inoltre, potrebbe anche ledere l’immagine e la reputazione aziendale.

10.2 Non inviare risposte ad e-mail che richiedano dati

Il dipendente non deve rispondere a messaggi di posta elettronica che richiedano l’autenticazione con le proprie credenziale di accesso all’account aziendale, ovvero che richiedano dati personali, credenziali di accesso, numeri di carta di credito, altre informazioni correlate al dipendente.

Si avvisa, infatti, il dipendente che allo stato attuale nessuna Amministratore di Servizi o Ente Pubblico o società privata (a titolo esemplificativo banche, Agenzia delle Entrate, Poste Italiane e simili) richiede tramite e-mail tali dati.

Pertanto, le eventuali richieste pervenute a mezzo mail sono da intendersi come richieste truffaldine e si richiede quindi la massima accortezza.

10.3 Non aprire allegati anche se provengono da mittenti noti

Il dipendente non deve aprire allegati non attesi o il cui invio non sia stato concordato con il mittente in quanto gli allegati sono mezzi attraverso cui vengono veicolati virus informatici o programmi che permettono a terzi di entrare nel sistema.

Prima di aprire qualsiasi allegato il dipendente è tenuto ad effettuare una scansione preventiva utilizzando l'antivirus.

10.4 Verificare sempre ortografia e sintassi nel testo delle e-mail ricevute

Il dipendente deve prestare attenzione al testo delle e-mail al fine di verificare la presenza di errori di ortografia, sintassi, traduzioni dall'inglese che risultano approssimative.

Nel caso in cui nel testo di una e-mail ricevuta si rilevino tali imprecisioni il dipendente deve prestare la massima attenzione in quanto potrebbe trattarsi di e-mail standard che vengono inviate contemporaneamente a milioni di potenziali vittime.

10.5 Diffidare di e-mail che mettono urgenza, che minacciano sanzioni, che promettono premi e vincite o che contengono richieste di aiuto

Il dipendente deve prestare attenzione e diffidare di e-mail il cui contenuto richiede l'apertura di un link o di un allegato minacciando un imminente pericolo (es.: la perdita di denaro o la chiusura di servizi).

Il dipendente, pertanto, non deve rispondere ad e-mail che minacciano sanzioni, che annunciano premi, che chiedono di fare qualcosa con urgenza, che contengono richieste di aiuto umanitario e simili.

10.6 Non cliccare su link contenuti sul corpo delle e-mail

Il dipendente non deve cliccare su collegamenti contenuti nel testo di e-mail inattese in quanto tale link può condurre a siti web capaci di carpire informazioni o infettare il computer.

Il dipendente deve inoltre prestare particolare attenzione ai collegamenti a siti web che richiedono informazioni personali, anche se l'e-mail sembra provenire da una fonte legittima, perché i siti web di phishing sono spesso repliche esatte di siti web legittimi.

10.7 Segnalare immediatamente l'incidente

In caso di apertura di e-mail / link / allegati sospetti il dipendente deve informare subito, in maniera circostanziata, l'UOS Sistemi Informativi della avvenuta fuoriuscita di dati all'esterno.

Se il dipendente sospetta di aver comunicato le credenziali ad un sito truffaldino è necessario che egli cambi immediatamente la password utilizzando un dispositivo diverso,

avvisando immediatamente l'UOS Sistemi Informativi.

Il dipendente deve usare sempre password univoche, di lunghezza adeguata, composte da caratteri minuscoli, maiuscoli, numerici e speciali; evitando di inserire nelle password riferimenti personali.

10.8 Comportamento da adottare nei casi dubbi

Nel caso in cui il dipendente riceva e-mail di contenuto sospetto, il miglior modo di agire è quello di non rispondere, non aprire allegati, non cliccare su link, non inoltrare la e-mail a colleghi ed avvertire l'UOS Sistemi Informativi.

Se dalle verifiche effettuate, la mail risultasse essere un tentativo di phishing o contenere un allegato malevolo, è necessario avvisare tempestivamente l'UOS Sistemi Informativi.

10.9 Diffidare anche di mittenti noti

Potrebbe verificarsi la circostanza che le e-mail truffaldine provengano da mittenti noti, da account dell'Azienda, da "uffici" della stessa, da una "assistenza tecnica", dal "gestore dell'account", da "gestore del server" di posta elettronica e simili.

Diffidare da comunicazioni che sembrano provenire dall'Azienda stessa e che segnalano problemi con il vostro account o le vostre credenziali.

Nel dubbio il dipendente deve contattare direttamente la struttura da cui sembra provenire il messaggio e chiedere chiarimenti.

Non inserire mai credenziali di autenticazione su siti raggiunti cliccando nel corpo di una e-mail.

Controllare sempre il reale indirizzo del mittente, spesso vengono utilizzati falsi domini simili agli originali.

Porsi la domanda: è plausibile che questo mittente mi contatti a questo indirizzo o che riceva questa mail?

10.10 allegati-mail personalizzate

Si avvisa il dipendente che l'e-mail ingannevole potrebbe anche essere personalizzata con informazioni relative all'ufficio o alla persona stessa del dipendente. Tali informazioni si possono reperire agevolmente sui social network o da elenchi pubblici, pertanto, anche se la e-mail dovesse sembrare realmente diretta al dipendente, è necessario mantenere alta l'attenzione e avvisare l'UOS Sistemi Informativi.

11. IMPLEMENTAZIONI DEL SISTEMA INFORMATICO

L'UOS Sistemi Informativi per sua natura si mantiene aggiornata attraverso la sperimentazione di software e hardware e sopraintende al buon funzionamento e alla sicurezza

del Sistema Informatico, al complesso dei beni e alle procedure informatiche.

La sicurezza e la gestibilità del Sistema Informatico sono legate alla sua omogeneità e coerenza.

L'UOS Sistemi Informativi è autorizzata ad intraprendere tutte le azioni di razionalizzazione, semplificazione e gestione del Sistema Informatico ai fini della sicurezza, disponibilità e gestibilità.

Ogni variazione del Sistema Informatico comporta valutazioni tecniche di fattibilità, opportunità, integrabilità e di sicurezza da parte dell'UOS Sistemi Informativi; pertanto mentre le acquisizioni di nuovi beni o procedure informatiche, possono di volta in volta trovare copertura in conti di costo di specifici settori/servizi, è l'UOS Sistemi Informativi che le approva, e le organizza sulla scorta dei criteri summenzionati.

Le necessità di variazione del Sistema Informatico devono sempre essere portate all'attenzione dell'UOS Sistemi Informativi, per tempo e comunque prima di intraprendere qualsiasi altra attività.

Le richieste di variazioni dei singoli utenti relative a configurazioni dei P.C. o permessi sui sistemi centralizzati di sicurezza, devono essere debitamente motivate e autorizzate dalla Direzione di riferimento.