Durante l'attività di smart working (lavoro agile) il dipendente ha l'obbligo di rispettare tutti i regolamenti, le policy, le direttive, i codici di comportamento aziendali in vigore all'atto dello svolgimento dell'attività stessa.
Ogni strumento di lavoro (es. dispositivi, software, portali, …) messo a disposizione durante l'attività di smart working, eventualmente messo a disposizione dall'Azienda, deve essere utilizzato con la massima cura, sia in termini di tenuta e conservazione (dispositivi), sia con rifermento alle modalità di accesso e al trattamento dati. Rimangono valide ed efficaci per tutti i dipendenti in "smart working" le nomine a persona autorizzata al trattamento dei dati ai sensi del Regolamento 2016/679/EU e dell'art. 2 – quaterdecies del D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018, già conferite, così come le istruzioni con esse fornite nonché le misure di sicurezza attivate dall'Azienda e specificate nei regolamenti interni e nelle procedure aziendali.
Le utenze VPN saranno disabilitate dal SIETC una volta che la modalità di accesso in Smart Working sia ritenuta non più operativa per l'utente interessato.
Qualsiasi eccezioni alle regole di accesso in modalità VPN ed in smart working viene autorizzata direttamente dal Titolare dei dati a cui saranno sottoposte le singole richieste con le relative motivazioni. Una volta ricevuta le autorizzazioni il SIETC può procedere al rilascio dei relativi accessi.

Comportamenti specifici

Si rappresentano, di seguito, i principali comportamenti rientranti nell'ambito del presente regolamento che tutti gli utenti che effettuano l'attività lavorativa in smart working devono attuare al fine di tutelare se stessi e l'Azienda Ospedaliero Universitaria Sant'Andrea. In relazione alle diverse configurazioni possibili, caratterizzate dai diversi strumenti utilizzati, è necessario adottare comportamenti differenti, ma sempre coerenti con il principio di minimizzazione dei rischi correlati alla sicurezza informatica e con l'attuale normativa in ambito privacy.

Configurazioni possibili:

a) Utilizzo servizi/portali pubblicati su internet, senza VPN e postazione di lavoro personale
b) Utilizzo di servizi/portali con VPN e postazione di lavoro personale
c) Utilizzo di servizi/portali con VPN e postazione di lavoro aziendale

Per ciascuna delle configurazioni precedentemente definite si riportano quindi le principali regole che devono necessariamente essere seguite dagli utenti. Eventuali comportamenti difformi ricadranno direttamente sotto la responsabilità degli utenti stessi con tutte le eventuali conseguenze civili e penali correlate. Giova ricordare in questa circostanza che un'eventuale compromissione della sicurezza informatica aziendale potrebbe comportare gravissime conseguenze sia in termini di continuità dei servizi erogati (amministrativi e sanitari) sia in termini di protezione dei dati aziendali, personali e/o sensibili trattati.

Utilizzo servizi/portali pubblicati su internet, senza VPN e postazione di lavoro personale

Per l'utilizzo della postazione di lavoro personale è necessario:

1. che sia dotata di sistema operativo aggiornato all'ultima release emessa dal produttore con installate le patch di sicurezza rilasciate dallo stesso, i sistemi operativi dichiarati a fine supporto (end of support) si suggerisce di non utilizzarli.
2. Che sia dotata dotata di software antivirus aggiornato.
3. Che sia sottoposta a scansione antivirus prima dell'utilizzo come postazione di smart working.

Durante lo svolgimento dell'attività lavorativa in modalità smart working l'utente è autorizzato a memorizzare sul dispositivo personale eventuali file esclusivamente per il tempo strettamente necessario alla loro elaborazione; tale tempo non deve mai eccedere la sessione di lavoro quotidiana. Terminata la sessione di lavoro quotidiana tutti i file eventualmente presenti all'interno del dispositivo personale devono essere cancellati.
Nel caso si dovessero utilizzare/elaborare file per un periodo di tempo superiore alla sessione di lavoro quotidiana, gli stessi (file) devono essere trasferiti all'interno dello spazio messo a disposizione dell'utente all'interno della piattaforma "AOUSA Cloud" raggiungibile al seguente indirizzo https://cloud.ospedalesantandrea.it.
È severamente vietato trasferire all'interno del cloud e all'interno della postazione di lavoro dati appartenenti a categorie particolari e nello specifico dati relativi alla salute dei pazienti.

La richiesta di abilitazione all' accesso a AOUSA Cloud deve pervenire tramite nota protocollata alla UOC SIeTC opportunatamente motivata e autorizzata dal Responsabile UO di appartenenza.
È vietata la detenzione sulle postazioni di lavoro di documentazione inerente all'attività lavorativa che violi il D.lgs. 101/2018 che adegua il Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196) alle disposizioni del Regolamento (UE) 2016/679.
L'utente è tenuto a garantire la riservatezza delle informazioni trattate non consentendo quindi l'accesso alle stesse da parte di soggetti terzi, quali eventuali altri utilizzatori del dispositivo personale o fornitori di servizi di archiviazione remota (es. servizi di backup o archiviazione online).
È vietato memorizzare sul dispositivo personale le credenziali di autenticazione ai sistemi dell'amministrazione o ad altri sistemi utilizzati per svolgere l'attività lavorativa.
Eventuali disservizi, compromissione dei dati contenuti o rotture della postazione di lavoro personale utilizzata per smart working ricadono sotto la responsabilità dell'utente stesso; l'Azienda declina ogni responsabilità per gli eventi precedentemente citati e non è tenuta ad intervenire per ripristinare o sostituire la postazione di lavoro e nemmeno ad effettuare eventuali risarcimenti danni correlati.
Eventuali costi correlati alla connettività per l'acceso ad internet sono a carico del dipendente.
Di seguito alcuni esempi di servizi/portali pubblicati su internet:

- Posta elettronica aziendale: https://webmail.ospedalesantandrea.it/
- Portale ANAC.

L'accesso al servizio di helpdesk è possibile inviando un'email al seguente indirizzo helpdeskrti@ospedalesantandrea.it.

Utilizzo di servizi/portali con VPN e postazione di lavoro personale

La postazione di lavoro personale può essere utilizzata come postazione di smart working esclusivamente se:

1. Dotata di sistema operativo aggiornato all'ultima release emessa dal produttore con installate le patch di sicurezza rilasciate dallo stesso , i sistemi operativi dichiarati a fine supporto (end of support) non potranno essere autorizzati alla connessione in rete.
2. Dotata di software antivirus aggiornato.
3. Sottoposta a scansione antivirus prima dell'utilizzo come postazione di smart working.

Durante lo svolgimento dell'attività lavorativa in modalità smart working l'utente è autorizzato a memorizzare sul dispositivo personale eventuali file esclusivamente per il tempo strettamente necessario alla loro elaborazione; tale tempo non deve mai eccedere la sessione di lavoro quotidiana. Terminata la sessione di lavoro quotidiana tutti i file eventualmente presenti all'interno del dispositivo personale devono essere cancellati. Nel caso si dovessero utilizzare/elaborare file per un periodo di tempo superiore alla sessione di lavoro quotidiana, gli stessi (file) devono essere trasferiti all'interno dello spazio messo a disposizione all'interno della piattaforma "AOUSA Cloud" raggiungibile al seguente indirizzo https://cloud.ospedalesantandrea.it.
È severamente vietato trasferire all'interno del cloud e all'interno della postazione di lavoro dati appartenenti a categorie particolari e nello specifico dati relativi alla salute dei pazienti. È vietata la detenzione sulle postazioni di lavoro di documentazione inerente all'attività lavorativa che violi il Regolamento (UE) 2016/679 ed il D. Lgs. 196/2003 come modificato dal D.Lgs. 101/2018.
La richiesta di abilitazione all' accesso a AOUSA Cloud deve pervenire tramite nota protocollata alla UOC SIeTC opportunatamente motivata e autorizzata dal Responsabile UO di appartenenza.
L'utente è tenuto a garantire la riservatezza delle informazioni trattate non consentendo quindi l'accesso alle stesse da parte di soggetti terzi, quali eventuali altri utilizzatori del dispositivo personale o fornitori di servizi di archiviazione remota (es. servizi di backup o archiviazione online).
È vietato memorizzare sul dispositivo personale le credenziali di autenticazione ai sistemi dell'amministrazione o ad altri sistemi utilizzati per svolgere l'attività lavorativa.
Eventuali disservizi, compromissione dei dati contenuti o rotture della postazione di lavoro personale utilizzata per smart working ricadono sotto la responsabilità dell'utente stesso; l'Azienda declina ogni responsabilità per

gli eventi precedentemente citati e non è tenuta ad intervenire per ripristinare o sostituire la postazione di lavoro e nemmeno ad effettuare eventuali risarcimenti danni correlati.
Eventuali costi correlati alla connettività per l'acceso ad internet sono a carico del dipendente.
In questa configurazione l'utilizzo della VPN è limitato esclusivamente al raggiungimento di specifici servizi web disponibili all'interno della rete aziendale e non consentirà di raggiungere altre risorse all'interno della rete stessa (es. cartelle condivise).

Di seguito alcuni esempi di servizi web disponibili all'interno della rete aziendale:

- Intranet Aziendale - default
- Portale Invio segnalazioni - default
- Portale Area Personale – default
- Portale Unica (Protocollo e Provvedimenti) – su richiesta
- AMC Master – su richiesta
- Privacy Manager.

L'accesso al servizio di helpdesk è possibile utilizzando il pulsante "Invio segnalazioni" presente all'interno della Intranet aziendale.

Utilizzo di servizi/portali con VPN e postazione di lavoro aziendale

L'utilizzo della postazione di lavoro aziendale, configurata al fine di garantire l'adeguato livello di sicurezza, consente l'accesso al proprio PC aziendale via Desktop Remoto. Questa configurazione permette quindi all'utente di avere a disposizione tutti gli strumenti di lavoro che avrebbe direttamente dalla scrivania del proprio ufficio; in questo contesto il lavoro svolto deve restare confinato all'interno degli strumenti di lavoro aziendali.
Durante lo svolgimento dell'attività lavorativa in modalità smart working l'utente è autorizzato a memorizzare sul dispositivo aziendale eventuali file esclusivamente per il tempo strettamente necessario alla loro elaborazione; tale tempo non deve mai eccedere la sessione di lavoro quotidiana. Terminata la sessione di lavoro quotidiana tutti i file eventualmente presenti all'interno del dispositivo aziendale devono essere trasferiti sulle risorse disponibili all'interno della rete aziendale (es. cartelle condivise).
È vietata la detenzione sulle postazioni di lavoro di documentazione inerente all'attività lavorativa che violi il D.lgs. 101/2018 che adegua il Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196) alle disposizioni del Regolamento (UE) 2016/679.
Eventuali costi correlati alla connettività per l'acceso ad internet sono a carico del dipendente.
L'accesso al servizio di helpdesk è possibile utilizzando il pulsante "Invio segnalazioni" presente all'interno della Intranet aziendale.
L'utente è tenuto a conservare e custodire con la massima cura il dispositivo aziendale ricevuto e ad utilizzarlo esclusivamente per fini aziendali; qualsiasi malfunzionamento, danno da uso improprio o furto sono a carico dell'utente stesso.

Ulteriori misure di sicurezza da adottare durante lo svolgimento dell'attività lavorativa in modalità "smart working"

Durante tutte le operazioni di trattamento (raccolta, elaborazione, archiviazione, diffusione dei dati, ecc.), le informazioni messe a disposizione dall'Azienda devono essere conservate con la massima diligenza. Ogni documento, sia esso in formato elettronico che cartaceo, deve essere gestito garantendo un livello di sicurezza adeguato ad evitare il rischio di violazione dei dati (intendendosi per tale la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati). Tale rischio sussiste, infatti, sia nell'utilizzo di apparati di servizio informatici e telematici, sia nel caso di documenti cartacei.
Il dipendente deve garantire la riservatezza di tutte le informazioni di cui venga a conoscenza per il lavoro assegnatogli nonché di quelle derivanti dall'utilizzo delle apparecchiature, dei programmi e dei dati in essi contenuti.
L'utente deve adottare i seguenti comportamenti sia in relazione all'utilizzo di strumenti tecnici ed informatici di proprietà sia nel caso di utilizzo/accesso di strumenti messi a disposizione dall'Azienda, eventualmente anche mediante i primi, e segnatamente:

1. Collegarsi alla rete aziendale con le modalità sopra descritte, impedendo l'accesso ad altri soggetti non autorizzati (es. coniuge, parenti, amici).
2. In fase di avvio del PC devono sempre essere richieste le credenziali di accesso (no login automatico).
3. Le credenziali di accesso (username e password) devono essere conservate con diligenza, in modo che restino riservate, evitando che terzi non autorizzati possano conoscerle. Deve essere utilizzata una password di almeno 8 caratteri alfanumerici, priva di riferimenti personali facili da indovinare (es. nome, cognome, data di nascita, ecc.), contenente almeno tre delle seguenti quattro tipologie di caratteri: lettere maiuscole, lettere minuscole, numeri, caratteri speciali (es. # @ ! ? . ,) Il computer ed eventuali altri strumenti in dotazione (smartphone, tablet, ecc.) non devono essere lasciati incustoditi e resi accessibili a persone non autorizzate. Nel caso del computer, l'utente è tenuto a disconnettere di volta in volta la sessione di lavoro, bloccando l'operatività del computer ed impedendo in tal modo indebiti accessi e/o visualizzazioni, anche solo accidentali, a persone non autorizzate.
4. Devono essere adottate tutte le misure necessarie ad evitare un utilizzo fraudolento o comunque non autorizzato della posta elettronica aziendale. L'accesso alla propria casella al di fuori della rete aziendale deve avvenire con le seguenti modalità: utilizzando webmail va sempre evitato il salvataggio delle credenziali di accesso proposto dal browser, in ogni caso al termine della sessione di utilizzo procedere con la disconnessione effettuando il "logout".
5. La persona autorizzata non deve mai utilizzare dispositivi esterni di memorizzazione (esempio: chiavette usb, hard disk esterni, ecc.).
6. Qualora sia stato fornito dall'Azienda un pc portatile, salvaguardare adeguatamente lo strumento messo a disposizione per la connessione nonché i dati eventualmente in esso contenuti, evitando di lasciarlo incustodito presso e al di fuori del domicilio (es. nel transito dal domicilio alla sede del servizio) ed evitarne l'utilizzo per finalità personali, inserendo documenti e dati attinenti la propria sfera privata. Si ricorda, infatti, che tale pc è uno strumento di lavoro fornito dal datore di lavoro.

Il dipendente deve inoltre attenersi alle seguenti ulteriori istruzioni. Deve in particolare:

- Evitare che le conversazioni telefoniche di lavoro vengano ascoltate, anche involontariamente, da soggetti non autorizzati (es. coniuge, parenti, amici, conoscenti, estranei, ecc.);
- Evitare di detenere al domicilio documentazione cartacea contenente dati personali di cui l'Azienda è Titolare, a meno che ciò risulti indispensabile nell'ambito della gestione dell'emergenza epidemiologica e/o nello svolgimento delle proprie attività istituzionali e, in tal caso, garantirne una custodia adeguata ad impedire ogni possibile contatto, anche accidentale, tra i dati personali e persone non autorizzate, nonché adottare ogni misura di sicurezza utile a minimizzare i rischi di distruzione, perdita, modifica, divulgazione non autorizzata. Quando sia strettamente necessario trasportare da un luogo ad un altro (mediante mezzi pubblici o privati, o anche a piedi) documenti contenenti dati, gli stessi devono essere raccolti in porta documenti, riportanti l'identificazione del dipendente ed un suo recapito;
- Qualora sia necessario cestinare documenti cartacei, renderli per quanto possibile illeggibili strappando ad esempio più volte la carta, in modo che i contenuti diventino indecifrabili e non ricostruibili.

Si rende, infine, necessario adottare nello svolgimento dell'attività precise cautele, volte a prevenire, oltre che a limitare al massimo, il possibile rischio di violazioni di dati personali. In tale ottica, la persona autorizzata si impegna a segnalare tempestivamente qualunque evento relativo a casi di violazione di dati personali (cd. data breach), al Titolare del trattamento per il tramite del proprio Delegato Privacy.
L'obbligo di segnalare senza indugio qualunque violazione di dati sussiste al fine di attivare le eventuali azioni conseguenti e necessarie, sulla base di quanto stabilito nella procedura aziendale di data breach e degli obblighi dal Regolamento (UE) 2016/679 e dal D.Lgs. 196/2003 come modificato dal D. Lgs.101/2018.

Accettazione del regolamento

Il presente regolamento, comprese eventuali sue revisioni, è automaticamente considerato accettato dall'utente dal momento di inizio delle attività in modalità smart working (lavoro agile).