SERVIZIO SANITARIO REGIONALE
Dipartimento Tutela della Salute e Politiche Sanitarie

AZIENDA OSPEDALIERA
"Annunziata – Mariano Santo S. Barbara"
Cosenza

REGIONE CALABRIA

Linee guida
per l'utilizzo delle risorse informatiche, di rete e software

Linee guida per l'utilizzo delle risorse informatiche, di rete e software	
Redatto da:	Ing. Maria Elena Cavaliere
Approvato con:	Deliberazione n. 417 del 20.9.2017

1. Introduzione

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer, espone l'Azienda Ospedaliera di Cosenza (AO) ai rischi di un coinvolgimento sia patrimoniale che penale, creando problemi alla sicurezza ed all'immagine dell'AO stessa. Premesso quindi, che l'utilizzo delle risorse informatiche e telematiche della nostra AO deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, l'AO ravvisa la necessità di definire delle linee guida dirette ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza dei dati.

Ciò considerato, l'Azienda Ospedaliera sta proseguendo altresì il percorso di perfezionamento delle procedure privacy, con un'azione decisa e costante nell'applicazione del disposto normativo di riferimento (Codice in materia di protezione dei dati personali) che prevede espresse direttive in materia di sicurezza con gli artt.31-36 e nell'Allegato B al Codice.

Tali linee guida, quindi, oltre a prevenire l'uso improprio delle nuove tecnologie da parte del personale impiegato, mirano altresì a prevenire un fenomeno in costante crescita come i "data breach".

I "data breaches" riguardano essenzialmente il concetto di violazione dei dati personali, consistente in un'attività che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la rivelazione non autorizzata di dati personali o l'accesso, sempre non autorizzato, di dati trasmessi, memorizzati o elaborati.

2. Finalità

Il presente documento definisce le corrette modalità circa l'accesso e l'utilizzo delle infrastrutture e delle risorse informatiche dell'AO:

- Computer e programmi aziendali
- Posta elettronica
- Rete internet

Le indicazioni riportate, si applicano a tutto il personale che opera all'interno dell'AO mediante l'ausilio di supporti informatici ed in generale a tutti coloro a cui, a qualsiasi titolo,

sia concesso l'uso delle risorse informatiche aziendali, sia controllate individualmente che condivise, gestite su un singolo computer o rese disponibili in rete.

Si rendono quindi necessarie delle linee guida al fine di garantire la sicurezza dei sistemi e del patrimonio informativo dell'AO.

L'adozione di queste indicazioni viene attuata nell'intento di:

- garantire la massima efficienza e sicurezza delle risorse informatiche e del loro utilizzo;
- garantire la riservatezza delle informazioni e dei dati;
- provvedere ad un servizio continuativo nell'interesse dell'Ente (attraverso procedure di disaster ricoveri e di back up);
- garantire il rispetto delle leggi in materia di utilizzo delle risorse informatiche;
- garantire la massima sicurezza nell'interazione tra l'Azienda Ospedaliera di Cosenza e altre istituzioni.

3. Risorse informatiche

I dispositivi hardware e software acquisiti, nonché la rete di trasmissione dati e tutti gli accessori ad essa collegati, l'elaborazione e la diffusione e comunicazione delle informazioni sia all'interno che all'esterno di essa, costituiscono strumenti indispensabili per la corretta gestione delle attività connesse alla mission aziendale.

L'AO assegna in uso al personale dispositivi ed attrezzature informatiche e ne promuove l'utilizzo ritenendole strategiche per le attività amministrative e di gestione dell'assistenza sanitaria.

Gli utenti della rete e delle risorse informatiche messe a disposizione dall'AO, sono tenuti a farne un corretto uso, ad averne cura e a seguire le indicazioni riportate nel presente documento.

4. Terminologia

Di seguito sono riportate le definizioni di alcuni termini utilizzati nel presente documento

- DATO PERSONALE, qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale
- DATO SENSIBILE, i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a

partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

- MISURE DI SICUREZZA, "misure minime", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;
- VIOLAZIONE DI DATI PERSONALI: violazione della sicurezza che comporta anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico;
- COMUNICAZIONE ELETTRONICA, ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un contraente o utente ricevente, identificato o identificabile;
- GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.
- CATENA DI S.ANTONIO: messaggio che induce il destinatario a produrne molteplici da spedire a nuovi destinatari.
- DOWNLOAD: scaricare, trasferimento dati sul PC.
- FILE SHARING: condivisione dei file.
- PEER TO PEER: architettura di rete caratterizzata da nodi equivalenti che possono sia usufruire da servizi che erogarne.
- LOG: registrazione sequenziale e cronologia delle operazioni effettuate , da un utente, un amministratore o automatizzazione, man mano che vengono eseguite dal sistema o applicazioni.
- PROXY SERVER: è un sistema che si interpone tra un client ed un server facendo da tramite o interfaccia, inoltrando le richieste e le risposte dall'uno all'altro.
- UTENTE: soggetto autorizzato con diritto di accesso ai servizi informatici e di rete.
- VPN: Virtual Private Network.

5. Utilizzo del personal computer fisso o mobile

Il personal computer, con annessi programmi e/o applicazioni affidati al dipendente sono strumenti di lavoro, pertanto vanno custoditi in maniera appropriata e il loro utilizzo può avvenire solo per scopi professionali (in relazione alle mansioni assegnate) e non anche per scopi personali.

Ogni utente è tenuto ad adottare, nell'ambito delle proprie attività, tutte le misure di sicurezza atte a prevenire la possibilità di accessi non autorizzati, furti, frodi, danneggiamenti, distruzioni o altri abusi nei confronti delle apparecchiature informatiche.

Per assicurare quanto sopra sono da evitare atti o comportamenti contrastanti con le predette indicazioni come, ad esempio, quelli appresso elencati indicativamente.

- Per prevenire il rischio concreto di introdurre virus informatici o di alterare la stabilità delle applicazioni dell'elaboratore, l'installazione di programmi provenienti dall'esterno deve essere espressamente autorizzata dall'Ufficio Informativo.
- E' vietato installare o prelevare software senza autorizzazione, copiare files eseguibili, mp3, giochi sia sui dischi di rete sia su quelli locali.
- E' espressamente vietato l'impiego di programmi non distribuiti ufficialmente dai produttori.
- Non è consentito usare software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici.
- Non è ammessa la modifica delle configurazioni impostate sul proprio personal computer.
- Non è consentita l'installazione sul personal computer di strumenti di comunicazione propri. (ad esempio modem).
- Il PC deve essere spento quotidianamente prima di lasciare i locali di lavoro o in caso di assenze prolungate. In ogni caso lasciare un PC acceso e incustodito connesso alla rete può essere causa di utilizzo improprio.
- Nel caso di PC condivisi in ambienti di lavoro (es. reparti), gli utenti sono chiamati ad una particolare attenzione alla chiusura della sessione di lavoro personale una volta ultimata l'attività lavorativa, al fine evitare trattamenti non consentiti e/o accessi non autorizzati.

- Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, (cd-rom, pen drive usb…)

6. Utilizzo della rete Internet

Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa.

Internet è uno strumento semplice ed economico per il trasferimento di informazioni ma è anche una fonte pericolosa di diffusione di virus informatici che possono colpire in breve tempo l'intera rete informatica aziendale.

- E' proibita la navigazione in Internet per motivi diversi da quelli funzionali all'attività lavorativa stessa.
- E' fatto divieto scaricare software di qualunque tipo (gratuito, freeware e shareware) prelevato da siti Internet, se non espressamente autorizzato dall'Ufficio Informativo.
- E' 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 o attinenti i compiti e le mansioni assegnate e con il rispetto delle normali procedure di acquisto.
- E' vietata la divulgazione sul web, compresi i social networks, di informazioni, foto e filmati che ritraggono pazienti, professionisti e ambienti dell'AO.
- In particolare per quanto riguarda i Social networks, è vietato divulgare notizie riguardanti l'AO che possano provocare pregiudizi e pubblicare foto o video la cui trasmissione possa avere ripercussioni negative.
- E' vietata la partecipazione a forum non professionali, l'utilizzo di chat lines (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi.
- Non è consentito inoltre la ricerca di documenti informatici e la navigazione nei siti con contenuti di natura oltraggiosa e/o discriminatoria per stato di salute/sesso/etnia/religione/opinione e/o appartenenza sindacale e/o politica.
- E' vietato accedere a siti ed acquisire o comunque diffondere prodotti informativi lesivi del comune senso del pudore;
- E' vietato diffondere prodotti informativi lesivi dell'onorabilità, individuali o collettivi;

- E' vietato diffondere, in rete o con qualsiasi altro mezzo di comunicazione, informazioni riservate di qualunque natura.
- E' vietato, ad ogni modo, ricercare, scaricare, trattare e diffondere qualsiasi informazione lesiva della dignità umana e/o informazioni non pertinenti con l'attività lavorativa.
- Non è consentito utilizzare software per il controllo remoto di altre risorse collegate alla rete. In particolare è vietato l'utilizzo di prodotti quali TeamViewer, PC_Anyware, Net_Meeting o similari senza espressa autorizzazione dell'Ufficio Informativo
- E' assolutamente vietato connettere alla rete macchine configurate con indirizzo IP statico, assegnato direttamente dall'utente, senza preventiva autorizzazione dei Servizi Informatici.
- Introdurre una macchina con un IP duplicato potrebbe causare un conflitto con l'indirizzo di un server oppure di un altro dispositivo della rete e causare gravi malfunzionamenti alla rete.
- Non è ammessa 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 necessari dovrà essere richiesto ai Servizi Informatici e ricevere autorizzazione.
- Analogamente non è ammesso l'utilizzo non autorizzato di dispositivi per lo sdoppiamento di punti di rete (mini HUB).
- E' fatto assoluto divieto di configurare servizi già messi a disposizione in modo centralizzato, quali ad esempio DNS; DHCP, proxy server.
- L'utilizzo di reti wireless deve essere autorizzato dai Servizi Informatici, nel caso di installazione nelle vicinanze di apparecchiature medicali, si dovrà valutare la compatibilità con le apparecchiature esistenti.
- Non è consentita la connessione di dispositivi privati alla rete aziendale
- gli accessi alla rete aziendale via VPN o meccanismi di tunneling analoghi sono vietati, a meno di casi da coordinarsi con i Servizi Informatici con le seguenti finalità:
    - assistenza software/sistemististica da parte di ditte esterne legate all'AO da un contratto di manutenzione;

- assistenza software/sistemistica da parte di personale dei Servizi Informatici;
- enti esteni all'AO che necessitano dell'utilizzo di procedure aziendali.

La navigazione in internet può formare oggetto di controllo, seppur graduale, rispettando i principi di liceità, pertinenza, necessità e non eccedenza (art.11 Codice in materia di protezione dei dati personali), tenendo conto anche delle linee guida del Garante per posta elettronica e internet. In particolare, al fine di verificare la funzionalità, la sicurezza del sistema ed il suo corretto utilizzo, le apparecchiature di rete preposte al collegamento verso internet, memorizzano i file di log contenente le informazioni relative ai siti che i pc aziendali hanno visitato.

7. Utilizzo della posta elettronica

La casella di posta, assegnata all'utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del loro corretto utilizzo.

L'utilizzo della posta elettronica è di uso esclusivamente personale e dovrà essere utilizzata dal soggetto individuato come utente e a cui sono riferite le credenziali di acceso, sotto la sua responsabilità. Pertanto le comunicazioni saranno considerate come riferibili al soggetto individuato come utente, sia dal punto di vista della provenienza che dei contenuti, salvo il caso in cui sia fornita prova che l'utilizzo del mezzo è avvenuto all'insaputa o contro la volontà del soggetto utente.

- E' vietato trasmettere e/o diffondere dati sanitari e altri dati sensibili da account di posta elettronica diversi da quelli aziendali.
- E' fatto divieto di utilizzare le caselle di posta elettronica @aocs.it per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-lists, inviare catene telematiche o di Sant'Antonio non attinenti la propria attività o funzione svolta per l'ente.
- Non è consentito inviare o memorizzare messaggi (interni ed esterni) di nature oltraggiosa, discriminatoria e in qualsiasi maniera lesiva della dignità umana.
- E' proibito aprire files eseguibili o documenti word ed excel ricevuti per posta elettronica di provenienza incerta, ovvero da enti e persone sconosciute perché potrebbero contenere virus informatici.

- La posta elettronica deve essere scaricata quotidianamente, onde evitare il blocco della corrispondenza.
- E' obbligatorio controllare con il software antivirus i file allegati di posta elettronica prima del loro utilizzo.
- Gli utenti sono tenuti a mantenersi aggiornati, controllando periodicamente le direttive comunicate.
- Non è consentito, ad ogni modo, inviare e/o memorizzare messaggi (interni o esterni) che non siano correlati con l'attività lavorativa del dipendente.
- E' fatto obbligo di comunicare con sollecitudine agli Uffici competenti eventuali comunicazioni e allegati che siano potenzialmente pericolosi per la sicurezza informatica e per il rispetto della dignità umana;
- Il dipendente che non consulta la posta elettronica aziendale è responsabile della mancata ricezione di informazione potenzialmente importanti per l'attività lavorativa.

Al singolo lavoratore sarà assegnato un indirizzo e-mail personale del tipo: nominativo@aocs.it. La personalizzazione dell'indirizzo non comporta la sua "privatezza", in quanto trattasi di strumenti di esclusiva proprietà dell'ente, messi a disposizione del dipendente al solo fine dello svolgimento delle proprie mansioni lavorative. I servizi di posta elettronica possono formare oggetto di analisi rispettando i principi di liceità, pertinenza, necessità e non eccedenza (art. 11 Codice in materia di protezione dei dati personali), tenendo conto anche delle linee guida del Garante per posta elettronica e internet.

Inoltre le singole strutture valuteranno l'opportunità di:

- attivare indirizzi di posta elettronica per le strutture, condivisi dagli operatori assegnati a ciascuna di esse (es struttura@aocs.it);
- rendere disponibili per ciascun lavoratore apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di assenze (ad esempio, ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un sostituto;
- consentire all'utente, in previsione della possibilità che in caso di assenza improvvisa o prolungata, si debba conoscere il contenuto dei messaggi di posta elettronica, di delegare un altro lavoratore (fiduciario) all'utilizzo della casella postale

8. Utilizzo della posta elettronica certificata (PEC)

L' Azienda Ospedaliera utilizza il servizio di Posta Elettronica Certificata (PEC) per la ricezione e la trasmissione di comunicazioni ufficiali.

In particolare:

- comunicazioni che necessitano di una ricevuta di accettazione e di consegna, la cui provenienza sia certa ai fini dei procedimenti amministrativi;
- documenti informatici la cui data ed ora di trasmissione e di ricezione siano opponibili a terzi;
- documenti informatici ed informazioni con soggetti interessati che ne fanno richiesta e che hanno preventivamente dichiarato il loro indirizzo di PEC.

9. Utilizzo della firma elettronica

L'utilizzo della firma digitale è personale ed il titolare è tenuto alla massima diligenza nella custodia sia del dispositivo di firma (smart card/OTP) che delle credenziali che ne consentono l' utilizzo (PIN) e risponde personalmente di qualunque uso improprio o fraudolento.

Per richiedere il rilascio del kit i Dirigenti devono recarsi personalmente presso l'Ufficio dei Servizi Informatici, muniti di tesserino del codice fiscale e documento di identità in corso di validità.

10. Protezione antivirus

- Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo.
- Ogni utente è tenuto a controllare il regolare funzionamento del software antivirus installato.
- Nel caso che il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente: sospendere ogni elaborazione in corso senza spegnere il computer e segnalare l'accaduto ai Servizi Infomatici.
- Non è consentito l'utilizzo di pc, floppy disk, cd/dvd, dvd riscrivibili, chiavi usb di cui non si conosce l'origine; Ogni dispositivo magnetico di provenienza esterna all'azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo.

11. Utilizzo dei supporti esterni di memorizzazione

Con le disposizioni del presente paragrafo sono descritti i comportamenti improntati alla prudenza e alla cautela, al fine di prevenire l'accesso da parte di soggetti non autorizzati ai dati personali contenuti nei dispositivi mobili e supporti rimovibili. L'utilizzo di tali strumentazioni si connota di un alto indice di criticità, in ragione della:

- natura dei dispositivi: i dispositivi mobili sono facilmente trasportabili ed occultabili;
- natura dei dati presenti sui dispositivi: sui dispositivi mobili possono essere presenti copie parziali e/o temporanee di dati personali o comunque di importanza strategica per la sicurezza dei sistemi;
- modalità di utilizzo dei dispositivi: i dispositivi mobili possono essere utilizzati in contesti diversi anche al di fuori di sedi dell'Ente ed in aree non sicure. Ciò rappresenta una minaccia per la sicurezza dei sistemi nel momento in cui, per esempio, un portatile si riconnette alla rete aziendale.

Inoltre:

- Non è consentito scaricare (download) archivi, programmi o dati contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria attività lavorativa.
- Non è consigliabile l'utilizzo di pen drive per il trasferimento di dati sui PC aziendali in quanto tali supporti potrebbero essere veicolo di virus.
- Occorre prestare particolare cautela nell'uso di piattaforme, funzionalità o spazi disco esterni all'AO (es Dropbox o Google Drive) per evitare accessi non autorizzati a dati riservati.

Per ciò che concerne la tutela dei dati sensibili e/o giudiziari, si prescrive di memorizzare in forma protetta i file che li contengono o che comunque possono compromettere la sicurezza dei sistemi informativi dell'AO (per es. proteggere l'accesso a cartelle o file tramite password, utilizzare appositi tool di cifratura concordandoli con il proprio referente informatico o con le strutture informatiche centrali, ecc.). Se non più utilizzati, si raccomanda di distruggere i supporti rimovibili contenenti dati sensibili e/o giudiziari, o rendere inintelligibili i dati in essi contenuti, impiegando strumenti preventivamente concordati con il proprio referente informatico o con le strutture informatiche centrali.

Le occasioni di furto, danneggiamento involontario, accesso non consentito ai dati contenuti nei dispositivi e comunque le situazioni di pericolo relative all'integrità dei dispositivi e dei dati, in ragione della portabilità degli stessi, sono considerevolmente maggiori rispetto alle postazioni di lavoro poste nelle sede dell'AO.

E' vietato lasciare incustoditi, in ogni caso, i dispositivi mobili, sia all'interno delle sedi dell'Ente sia all'esterno.

12. Unità Operativa Semplice Servizi Informatici

Tutto l'Hardware ed il Software potrà essere utilizzato solo previa richiesta di parere tecnico favorevole da parte dei Servizi Informatici, che controllerà, confrontandosi con il Responsabile privacy (figura obbligatoriamente prevista dal Nuovo Regolamento Europeo per la protezione dei dati personali), le richieste al fine di valutare la compatibilità con i Sistemi Informativi in essere e prevenire eventuali danneggiamenti.

Il lavoratore che, nell'espletamento delle proprie funzioni, riscontri difficoltà o dubbi in merito all'utilizzo di risorse informatiche, di rete e software, non dovrà adottare iniziative personali ma dovrà, invece, comunicare obbligatoriamente tale/i criticità ai Servizi Informatici che provvederà a fornire supporto all'utente.

Allo stesso spetta dunque la verifica tecnica della compatibilità degli strumenti elettronici con l'infrastruttura di rete e nel caso in cui gli strumenti proposti non possano, per ragioni tecniche, essere installati, saranno individuate, ove possibile e nei limiti della tecnologia, soluzioni alternative, tecnicamente fattibili ed economicamente valide d'intesa con il servizio richiedente.

In particolare, considerando che la rete dell'Azienda si basa su protocollo TCP/IP, tutte le apparecchiature connesse alla rete sono configurate per ricevere l'indirizzo IP assegnato staticamente esclusivamente dai Servizi Informatici, a seconda della tipologia di apparecchiatura.

13. Riferimenti Normativi

Decreto Legislativo 196 del 30/06/2003 – "Codice in materia di protezione dei dati personali";

Decreto Legislativo. 82 del 07/03/2005 – "Codice dell'amministrazione digitale";

Linee guida del Garante per posta elettronica e internet Gazzetta Ufficiale n.58 10 marzo 2007.

14. Conclusioni

Tali linee guida, suscettibili di aggiornamento, rappresentano, quindi, una ulteriore attività di sensibilizzazione in materia di sicurezza informatica e sotto il profilo della protezione dei dati personali posta in essere da questa AO.

L'organizzazione e l'implementazione delle misure da mettere in campo saranno individuate anche alla luce del Nuovo Regolamento Europeo per la protezione dei dati personali (che entrerà in pieno vigore dal 25 maggio 2018) e dei suoi principi fondanti: Privacy by Design , Privacy by Default e Valutazione di impatto privacy.

L'Azienda Ospedaliera, quindi, attribuisce particolare rilevanza alle Linee guida riportate nel presente documento, garantendo che tra la Direzione Strategica, i Servizi Informatici e il Responsabile privacy si lavori in maniera sinergica per raggiungere gli obiettivi imposti dal legislatore europeo.