SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Ospedaliero - Universitaria di Parma

FRONTESPIZIO DELIBERAZIONE

AOO: AOO000

REGISTRO: Deliberazione

NUMERO: 0000439

DATA: 28/06/2023 12:49

OGGETTO: Regolamento interaziendale per l'utilizzo dei sistemi informatici

SOTTOSCRITTO DIGITALMENTE DA:

Il presente atto è stato firmato digitalmente da Fabi Massimo in qualità di Direttore Generale
Con il parere favorevole di Rossi Sandra - Direttore Sanitario FF
Con il parere favorevole di Ventura Antonio - Direttore Amministrativo

Su proposta di Marco Brambilla - Servizio Interaziendale Tecnologie dell'Informazione che esprime parere favorevole in ordine ai contenuti sostanziali, formali e di legittimità del presente atto

CLASSIFICAZIONI:

- [01-03-01]

DESTINATARI:

- Collegio sindacale
- S.S. Medicina Legale

DOCUMENTI:

File	Firmato digitalmente da	Hash
DELI0000439_2023_delibera_firmata.pdf	Brambilla Marco; Fabi Massimo; Rossi Sandra; Ventura Antonio	FD0CCA0F6CB4B36F03D5F34633A8607617A78384DD51516B83ADAA2C73C37A09
DELI0000439_2023_Allegato1.pdf:		EF7EE0D7A80A990621DA5AE3143A80FDA40D5AD13E29CAC76126500D74F7E24C

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Ospedaliero - Universitaria di Parma

DELIBERAZIONE

OGGETTO: Regolamento interaziendale per l'utilizzo dei sistemi informatici

IL DIRETTORE GENERALE

VISTI:

- gli articoli 22, 23, 23-bis, 23-ter del Decreto Legislativo 7 marzo 2005, n. 82, "Codice dell' Amministrazione Digitale";
- Il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati;
- il Decreto Legistavo 30 giugno 2003, n. 196 recante "Codice in materia di protezione dei dati personali" come novellato dal Decreto Legislativo 10 Agosto 2018, n. 101 (Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regiolamento (UE) 2016/679)

RICHIAMATE le seguenti deliberazioni:

- n. 370 del 7 Aprile 2021 dell'Azienda Ospedaliero Universitaria di Parma, avente ad oggetto l'adozione del "Piano triennale ICT 2021 - 2023";
- n. 325 del 4 maggio 2022 con la quale si procedeva all'approvazione della "Relazione Piano ICT 2021" dell'Azienda Ospedaliero - Universitaria di Parma;
- n. 380 del 8 Settembre 2022 dell'Azienda USL di Parma e n. 632 del 14 settembre 2022 dell'Azienda Ospedaliero Universitaria di Parma, con cui le due Aziende Sanitarie si dotavano di un "Piano Triennale per la Transizione Digitale Interaziendale 2022-2024" e che assegnava al Servizio Interaziendale Tecnologie dell'Informazione, nell'ambito delle attività di Sicurezza Informatica perseguite, il compito di proporre il Regolamento interaziendale dei sistemi informatici;
- n. 1007 del 23/12/2019 dell'Azieda USL di Parma e n. 1478 del 23/12/2019 dell'Azenda Ospedaliero Universitaria di Parma avente ad oggetto «Adozione del Manuale Aziendale in materia di trattamento dei dati personali"

RICHIAMATO altresì l'atto n. 108 del 15 marzo 2016 con il quale è stato approvato il Regolamento per l' utilizzo dei sistemi informatici dell'Azienda Ospedaliero – Universitaria di Parma;

CONSTATATO che il Servizio Interaziendale tecnologie dell'Informazione, come definito nel "Piano Triennale per la Transizione Digitale Interaziendale 2022/2024", ha ritenuto di interesse aziendale elaborare un Regolamento interaziendale di utilizzo dei Sistemi Informatici delle due Aziende Sanitarie in linea con il "Codice dell'Amministrazione Digitale" che diffonda a tutto il personale le corrette modalità di utilizzo degli strumenti Informatici forniti dall'Azienda ai propri collaboratori per lo svolgimento delle mansioni e compiti affidati e di utilizzo dello strumento della posta elettronica (email) così come indicato " 4.2 Posta elettronica";

DATO ATTO che l'informazione e condivisione preventiva è stata realizzata nei confronti di tutta le rappresentanze sindacali a partire dalla nota prot. 17961 del 27/04/2023 dell'Azienda Ospedaliero Universitaria di Parma a cui hanno fatto seguito gli incontri con le OOSS del 4, 8, 17, 25 Maggio 2023;

DATO ATTO che il presente provvedimento non comporta oneri di spesa diretti;

Delibera

Per le motivazioni esposte in premessa:

1. di approvare il "Regolamento interaziendale per l'utilizzo dei sistemi informatici", allegato al presente atto di cui costituisce parte integrante;
2. di diffondere tramite la rete intranet l'adozione del Regolamento interaziendale per l'utilizzo dei sistemi informatici;
3. di dare atto che il presente provvedimento non comporta oneri di spesa diretti.

Responsabile del procedimento ai sensi della L. 241/90:
Marco Brambilla

Regolamento interaziendale per l'utilizzo dei sistemi informatici
Azienda Ospedaliero – Universitaria di Parma
Azienda USL di Parma

Indice

1. Premessa

Le realtà aziendali sono andate caratterizzandosi in questi ultimi anni per l'elevato uso delle tecnologie informatiche che, se da un lato hanno consentito l'introduzione di innovative tecniche di gestione dell'azienda, dall'altro hanno anche dato origine a numerose problematiche relative all'utilizzo degli strumenti informatici forniti dall'azienda ai propri collaboratori per lo svolgimento delle mansioni e compiti affidati.

In questo senso, viene fortemente sentita dai datori di lavoro la necessità di porre in essere adeguati sistemi di verifica sull'utilizzo di tali strumenti da parte dei dipendenti/collaboratori e di sanzionare conseguentemente quegli usi scorretti che, oltre ad esporre l'azienda stessa a rischi tanto patrimoniali quanto penali, possono di per sé considerarsi contrari ai doveri di diligenza e fedeltà previsti dagli artt. 2104 e 2105 del Codice civile.

I controlli sull'uso degli strumenti informatici, tuttavia, devono garantire tanto il diritto del datore di lavoro di proteggere la propria organizzazione, essendo i computer aziendali strumenti di lavoro la cui utilizzazione personale è preclusa, quanto il diritto del lavoratore a non vedere invasa la propria sfera personale, e quindi il diritto alla riservatezza ed alla dignità come sanciti dallo Statuto dei lavoratori e dalla normativa relativa alla protezione dei dati personali (Reg. 2016/679/UE, c.d GDPR e D.lgs. 196/2003 e ss.mm.ii., c.d. Codice Privacy).

Il presente regolamento, pertanto oltre a dettare una disciplina per l'utilizzo degli strumenti informatici interaziendali, vuole costituire un utile strumento per sensibilizzare il personale su altri aspetti altrettanto importanti nella gestione dei sistemi informatici aziendali, quali il rispetto della normativa sulla tutela legale del software (e quindi il controllo sulla regolarità del software presente nello stesso sistema informatico), e quella sulla tutela del know-how aziendale, quando queste importanti informazioni di proprietà dell'impresa sono custodite nel sistema informatico.

Ogni utilizzatore dei sistemi informatici gestiti dal Servizio Interaziendale Tecnologie delle Informazioni (di seguito SITI) è tenuto a rispettare il presente Regolamento.

L'utilizzo degli strumenti informatici aziendali deve svolgersi nel rispetto della "privacy" degli interessati con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati.

Dal GDPR deriva una serie di obblighi in capo a chiunque utilizzi dati personali; non soltanto obblighi di riservatezza e segretezza ma anche di tutela, protezione e sicurezza degli stessi. La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet dai Personal Computer (di seguito anche PC), espongono le aziende sanitarie di Parma (di seguito AASS) e gli utenti (dipendenti e collaboratori delle stessa) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (sicurezza informatica, legge sul diritto d'autore, legge sul corretto trattamento dei dati...), creando evidenti problemi alla sicurezza ed all'immagine delle aziende stesse. Premesso quindi che l'utilizzo delle tecnologie dell'informazione deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, le AASS adottano questo regolamento diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

Il presente documento, che è stato redatto tenendo conto delle indicazioni contenuti nei provvedimenti AGID e del Garante per la protezione dei dati personali (nel prosieguo Garante), ha lo scopo di agevolare la lettura e l'interpretazione della normativa, dettando le necessarie prescrizioni e fornendo istruzioni operative.

Le istruzioni riportate si rifanno alla normativa in materia di protezione dei dati personali, alla normativa sul crimine informatico e più in generale al corpo normativo che disciplina i rapporti di lavoro.
Le aziende garantiscono che per nessuna ragione i dati informatizzati gestiti dall'azienda, i sistemi di elaborazione dati e gli strumenti di telecomunicazioni saranno utilizzati per il controllo a distanza dei lavoratori (artt. 113, 114 e 115 del Codice Privacy; artt. 4 e 8 l. 20 maggio 1970, n. 300) se non a fronte di specifica richiesta delle autorità competenti comprovanti un'attività d'indagine in corso.
La finalità è quella di regolamentare l'interazione tra persona fisica e strumenti informatici e dati trattati al fine di permettere un governo in sicurezza e liceità delle informazioni e dei processi delle AASS. Il raggiungimento di tale finalità si esplica anche attraverso la promozione, in tutti gli utenti, di una corretta "cultura informatica" affinché l'utilizzo degli strumenti informatici e telematici forniti dall'AASS, quali la posta elettronica, internet e i personal computer con i relativi software, sia conforme alle finalità e nel pieno rispetto della legge.

2. Campo di applicazione, entrata in vigore, transitorio

Il regolamento, così aggiornato, entra in vigore a distanza di 90 giorni dal momento della sua adozione. Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.
Copia del regolamento è pubblicato nella sezione SITI della intranet. Al momento della creazione dell'utenza da parte dei soggetti competenti (indicati al punto 4.1), questi consegnano copia del regolamento agli utenti.
Il regolamento si applica a tutti gli utenti del sistema informatico, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori delle aziende a prescindere dal rapporto contrattuale con la stessa intrattenuto se dotati di utenza del sistema stesso.
Ai fini del presente regolamento si intendono per strumenti (o risorse) informatici aziendali le dotazioni informatiche (hardware e/o software) acquisite, gestite e manutenute dal SITI nelle due AASS.
Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche per "utente" deve intendersi ogni dipendente e collaboratore (lavoratori somministrati, collaboratori coordinati e continuativi, in stage, agenti, dipendenti di fornitori eccetera) in possesso di specifiche credenziali di autenticazione. Nel seguito del presente documento, per semplicità espositiva, si farà riferimento genericamente all'operatore (o utente).
L'adozione di questo aggiornamento viene effettuato nell'intento di perseguire i seguenti scopi nell'ordine di priorità elencato:

- fornire la massima disponibilità ed efficienza del servizio nell'interesse della *mission* aziendale;
- garantire la massima sicurezza nell'accesso alla rete privata (Intranet) e pubblica (Internet);
- garantire il rispetto della normativa in materia di protezione dei dati personali e riservatezza (in senso lato, "Tutela della Privacy") attraverso un utilizzo lecito delle risorse informatiche per l'elaborazione di dati personali e sensibili;
- provvedere ad un'efficiente attività di monitoraggio e supervisione dei sistemi.

È comunque indispensabile che chiunque tratti dati personali segua le istruzioni derivanti dal GDPR e dalla sua applicazione all'interno delle AASS.
Le seguenti istruzioni sono parte del sistema di sicurezza che Azienda Ospedaliero-Universitaria e Azienda USL di Parma adottano al fine di gestire, nel rispetto della vigente normativa, il corretto funzionamento e manutenzione dei sistemi informatici gestiti dal SITI.
È fondamentale ricordare che nel sistema informatico aziendale si possono presentare interruzioni di servizio per numerose ragioni. La probabilità dell'accadimento di tali eventi, seppur riducibile aumentando l'affidabilità dei sistemi, non è mai nulla. Per questo motivo è compito dei singoli Delegati al Trattamento Dati procedere alla definizione di un piano di continuità d'emergenza da utilizzare in caso di fermo del sistema informatico che consenta l'erogazione del servizio e dia continuità alle funzioni organizzative.

3. Accesso al sistema informatico

3.1. Gestione ed assegnazione delle credenziali di autenticazione

Le credenziali di autenticazione per l'accesso al sistema informatico vengono assegnate alle diverse tipologie di persone che per svolgere il loro incarico debbano accedere al sistema informatico interaziendale. Le figure che le AASS hanno individuato aver diritto a credenziali di autenticazione al sistema informatico aziendale sono:

1. personale dipendente o diversamente inquadrato nelle varie forme previste contrattualmente (fonte Anagrafica del Dipartimento Risorse Umane);
2. personale a contratto (es. 15 *septies* D.lgs. 502 del 30 dicembre 1992 e ss.mm.ii.). e liberi professionisti (es. incarichi da selezioni…) (fonte Anagrafica del Dipartimento Risorse Umane);
3. personale in convenzione con l'Università degli Studi di Parma (fonte Anagrafica del Dipartimento Risorse Umane);
4. personale in formazione specialistica in convenzione con l'Università tramite appositi accordi con le AASS (fonte Anagrafica del Dipartimento Risorse Umane);
5. personale in tirocinio formativo o stage presso AASS;
6. personale dipendente di aziende fornitrici delle AASS e liberi professionisti con incarichi correlati a specifici servizi aziendali (es. Attività Tecniche, Affari Legali…);
7. personale dipendente di aziende (o associazioni) in convenzione con le AASS.

L'assegnazione delle credenziali avviene contestualmente all'inizio del rapporto nelle prime quattro figure. Sono quindi le articolazioni delle due AASS che alimentano l'Anagrafica delle Risorse Umane che consegnano credenziali e regolamento mentre per le figure ai punti 5, 6 e 7 avviene tramite la compilazione della modulistica da parte del tutor aziendale.
Il tutor aziendale è quella figura, dotata di credenziali di autenticazione e rientrante in una delle prime tre categorie, delegata/autorizzata al trattamento dati dal Titolare che ha la responsabilità rispetto alla persona per cui svolge il ruolo di tutor di:

- richiesta di credenziali previa verifica della necessità di accesso ai dati aziendali;
- consegna credenziali e regolamento alla persona fisica
- eventuale richiesta di accesso agli applicativi con relativa profilatura coerentemente alle prescrizioni aziendali in termini di trattamento del dato;
- disattivazione delle credenziali al venir meno della necessità di accesso.

Tipicamente per la figura del punto 5, il tutor, ai sensi del presente regolamento, è il medesimo tutor del tirocinio / stage nelle aziende; mentre per le figure dei punti 6 e 7 corrisponderà tipicamente con il responsabile unico del procedimento (o direttore dell'esecuzione) che ha in carico la gestione della fornitura/convenzione in oggetto.

Le richieste mediante modulistica vengono evase, di norma, entro 7gg lavorativi.

Per l'accesso al sistema informatico delle AASS ciascun utente deve essere in possesso della specifica credenziale di autenticazione.
Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id) associato ad una parola chiave (password) riservata che dovrà essere custodita dall'incaricato con la massima diligenza e non divulgata.

Il sistema gestisce complessità e durata delle password in modo dinamico: l'utente è tenuto al rispetto del sistema di controllo di complessità della password (ivi incluse le funzioni di non riuso di password già usate in precedenza).
Per la composizione e gestione della parola chiave (password), l'utente deve conformarsi alle seguenti prescrizioni ,

- la password deve essere abbastanza lunga, ovvero composta da un minimo di almeno 8 caratteri; si consiglia, comunque, di comporla con un numero maggiore di caratteri;
- la password contenga caratteri di almeno 3 tipologie diverse, tra cui lettere maiuscole e minuscole, numeri;
- la password non contenga dati o riferimenti personali identificativi, quali nome, cognome, data di nascita o una loro combinazione o ad altri riferimenti facilmente riconducibili all'utente;
- la password non contenga riferimenti al nome utente, mail, alias personale, user id o altri identificativi digitali;
- la password non contenga parole presenti in dizionari (italiani o altri);
- la password deve essere cambiata periodicamente;
- la password deve essere diversa da quella utilizzata per scopi personali (es. e-mail personale; social network…);
- la password non sia già stata utilizzata in passato;
- la password non deve essere scritta su post-it, blocchi note o biglietti che potrebbero essere smarriti o facilmente reperibili e visibili da soggetti terzi;
- la password non sia condivisa.

È necessario procedere alla modifica della parola chiave a cura dell'utente al primo utilizzo e, successivamente, almeno ogni novanta giorni.
Gli user-id non sono modificabili a richiesta dell'utente anche in caso di cambio di uno o più dati anagrafici, ad esempio nome, cognome o altro.
È facoltà dell'utente utilizzare lo strumento della domanda segreta per reimpostare la password nel caso, comunque considerato d'emergenza, di dimenticanza della stessa. È altresì facoltà dell'utente utilizzare gli strumenti di reset password avanzati che utilizzano canali alternativi (es. videocall). La validità delle credenziali d'accesso al sistema informatico è delimitata dalla validità del rapporto in essere con la persona fisica associata alle credenziali d'accesso. In particolare

ogni coppia di credenziali avrà validità per ulteriori 7 giorni al termine del rapporto che lega la persona fisica con le AASS.
Si evidenzia che in caso di lunga assenza (es. aspettativa, comando e sospensione del rapporto) l'account, con tutte le relative abilitazioni, rimane attivo.
È assolutamente proibito accedere al sistema informatico e nei programmi con un codice d'identificazione utente diverso da quello assegnato anche nel caso in cui all'interno del profilo utente siano custoditi documenti necessari all'espletamento di determinate attività aziendali. A tal proposito si ricorda che è cura e obbligo di ogni utente mettere a disposizione del proprio responsabile la documentazione aziendale da lui prodotta prima che il proprio account venga bloccato per scadenza del contratto.

3.2. Autenticazione degli utenti al sistema informatico aziendale

A tutti gli utenti del sistema informatico interaziendale è chiesto automaticamente, almeno ogni 90 giorni, il cambio della parola chiave. Tuttavia, qualora si ritenga che la stessa non sia più sicura, è consigliabile sostituirla anche prima di tale termine.
Qualora invece si utilizzino sottosistemi non in grado di richiedere automaticamente il cambio di password è indispensabile che l'utente – autonomamente - provveda a cambiarla, almeno ogni 90 giorni.
Gli utenti, autorizzati all'accesso al sistema informatico aziendale come sopra detto, sono responsabili di ogni utilizzo indebito o non consentito delle credenziali di cui sono titolari, così come anche della protezione dei dati utilizzati e/o memorizzati nei sistemi in cui hanno accesso.
Gli stessi sono tenuti a consultare la manualistica disponibile sul sito intranet riguardante l'utilizzo degli strumenti informatici dati in dotazione.

3.3. Richiesta, modifica e revoca delle abilitazioni ai sistemi informatici

Per la richiesta, la modifica e la revoca delle abilitazioni ai sistemi informatici è previsto l'utilizzo di uno strumento informatico. Tale strumento (c.d. "modulistica on line") prevede la dematerializzazione dei moduli di richiesta utilizzando, ai sensi del CAD (Codice dell'Amministrazione Digitale aggiornato con D.Lgs. 235/2010), la firma elettronica basata sugli strumenti di autenticazione del sistema informatico interaziendale (username e password).
In sintesi la persona che esegue l'accesso alla modulistica (usando username e password) è identificato come Responsabile della Richiesta (generalmente il Delegato al trattamento dei dati), mentre la persona che verrà identificata all'interno della modulistica sarà identificata come Richiedente al termine della compilazione sempre attraverso la propria username e password.
Per agevolare le operazioni di compilazione da parte del Responsabile della Richiesta sarà sempre possibile preparare uno o più moduli e rimandare la firma elettronica del Richiedente a quando, quest'ultimo, farà accesso al suo Cruscotto Personale (in cui il Richiedente dovrà usare la sua username e password per accedere).
Qualora il Responsabile della Richiesta non fosse un Delegato al Trattamento Dati ufficialmente incaricato dalla funzione Privacy, il sistema richiederà, durante il processo di identificazione del Richiedente, di individuare il Delegato al Trattamento Dati da cui si è stati delegati o incaricati per la compilazione della modulistica.

Per consentire un completa tracciatura delle richieste, il sistema prevede un invio di email ai vari attori coinvolti nel modulo compilato (responsabile della richiesta, richiedente ed eventuale delegato al trattamento dati).

4. Strumenti di comunicazione e condivisione delle informazioni
4.1. Internet

Le regole di seguito specificate sono adottate anche ai sensi delle "Linee guida del Garante per posta elettronica ed internet" pubblicate in Gazzetta Ufficiale n. 58 del 10/03/2007. Ciascun utente si deve attenere alle seguenti regole di utilizzo della rete internet e dei relativi sevizi.
E' vietato l'utilizzo personale e non istituzionale della connessione a internet., Tutti gli accessi ad Internet vengono registrati sul sistema di sicurezza aziendale in appositi file di log; tali log tengono traccia dei seguenti dati per ogni accesso:

- identificativo dell'utente (user id) che ha navigato in internet;
- indirizzo IP della stazione di lavoro;
- data e ora;
- riferimento al sito visitato (URL).

Tali log vengono conservati per un periodo massimo di 30 giorni dal SITI dopodiché vengono cancellati a meno di necessità esplicitate dall'autorità giudiziaria.
Tali log sono indispensabili per poter monitorare il corretto funzionamento del sistema nella sua globalità e per poter effettuare statistiche periodiche sull'uso del sistema. I log saranno trattati in maniera tale da fornire informazioni in maniera aggregata ed in modo da precludere l'immediata identificazione degli utenti, a meno che non vi siano specifiche ragioni di sicurezza informatica o richieste dall'autorità giudiziaria per accedere al dettaglio massimo, cioè alle informazioni di tipo nominativo.

Le aziende si riservano di filtrare l'accesso a siti che non risultino in relazione con le attività istituzionali; il filtraggio verrà attuato mediante l'inserimento dei siti non accessibili in una cosiddetta "Black list", ossia nell'inserimento del sito in una categorizzazione, eventualmente predisposta anche da fornitori esterni specializzati. Lo strumento non garantisce l'inaccessibilità a siti non istituzionali poiché i siti non ancora categorizzati sono per scelta visibili.
I delegati al trattamento o comunque il personale incaricato dal Titolare o dai delegati stessi, tramite l'apposita procedura visualizzabile anche sulla pagina di blocco, può richiedere la rimozione dalla lista di esclusione di un sito. L'accesso a siti web, considerati non istituzionali dal sistema di filtraggio ma coerenti con i principi della Direttiva del Ministro per la Pubblica Amministrazione e l'Innovazione del 26/05/2009 n. 2/09, è comunque possibile concordandone le modalità con il proprio responsabile. La richiesta sarà vagliata dal SITI che, valutandone gli aspetti tecnici, potrà accettare o rifiutare tale richiesta, motivandola.
Il servizio Internet non può essere utilizzato per scopi di lucro o per qualsiasi attività economica o per scopi non riconducibili ad attività istituzionale.
Non è permesso l'utilizzo di Software di Instant Messaging, Chat, telefonate virtuali (Skype e similari) e Stazioni Radio/Video via Internet, file sharing, download eccetera se non rientranti nei percorsi istituzionali aziendali, regionali o di enti sovraordinati.
Il servizio Internet non può essere comunque utilizzato per scopi vietati dalla legislazione vigente.
A titolo di esempio, senza che questo costituisca un elenco esaustivo, non è consentito:

- servirsi o dar modo ad altri di servirsi della stazione di accesso a Internet per attività poste in essere in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;
- utilizzare Internet Provider diversi da quello aziendale e la connessione di stazioni di lavoro aziendali alle reti di detti provider con sistemi di connessione diversi (es. modem) da quello centralizzato;
- usare la rete in modo difforme da quanto previsto dal presente documento e dalle leggi penali, civili e amministrative in materia di disciplina dell'attività e dei servizi svolti sulla rete;
- l'invio di dati personali o sensibili tramite la rete internet (Upload) se non preventivamente autorizzati dal Delegato al Trattamento dati e utilizzando gli opportuni accorgimenti di sicurezza (protocolli crittografati HTTPS/SSL, firma digitale eccetera);
- la memorizzazione/consultazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica
- la produzione e pubblicazione di propri siti e/o altri servizi Web sulla infrastruttura tecnologica delle AASS;
- la partecipazione a Forum non professionali, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Delegato al Trattamento;
- l'utilizzo di siti di social networking anche se per uso didattico, di ricerca o di interscambio di comunicazioni se non utilizzando eventuali account istituzionali aziendali.

4.2. Posta elettronica ed office automation

Le regole di seguito specificate sono adottate anche ai sensi delle "Linee guida del Garante per posta elettronica ed internet" pubblicate in Gazzetta Ufficiale n. 58 del 10/03/2007. Ciascun utente si deve attenere alle seguenti regole di utilizzo della rete internet e dei relativi sevizi.
La casella di posta elettronica assegnata all'utente è uno strumento di lavoro ed è vietato l'utilizzo personale e non istituzionale della posta elettronica aziendale. Valgono inoltre i seguenti punti:

- le persone assegnatarie delle caselle di posta elettronica (i.e. ncognome@ao.pr.it, ncognome@ausl.pr.it) sono responsabili del corretto utilizzo delle stesse;
- è dotato di casella di posta elettronica interaziendale il personale dipendente (strutturato o a contratto), precedentemente identificato ai punti 1, 2 e 3 del paragrafo "Gestione ed assegnazione delle credenziali di autenticazione". L'utilizzo e la consultazione della casella di posta elettronica sono un diritto e un dovere per il suddetto personale;
- non è prevista la creazione di mailbox condivise tra più utenti, a fronte di tali necessità sarà possibile creare una lista di distribuzione (vedi par. 5.3)
- il personale in formazione universitaria (specializzandi, borsisti relativi al punto 4 del precitato paragrafo) ha la possibilità di indicare il proprio indirizzo e-mail universitario personale (i.e. nome.cognome@unipr.it), tramite la modulistica, al fine del suo inserimento nella rubrica aziendale. A tal riguardo è bene evidenziare come

problematiche sul sistema di posta universitario possono compromettere la comunicazione nonostante l'inserimento degli indirizzi sulla rubrica interaziendale;

- il sistema di posta elettronica interaziendale non è un sistema di posta certificata; non vi è pertanto la garanzia della consegna o della ricezione dei messaggi di posta, né fornisce garanzia di riservatezza e sicurezza relativamente ai messaggi inviati in quanto non usa alcuna tecnica di crittografia dei contenuti o di protezione delle autenticazioni. È responsabilità del mittente selezionare il corretto strumento di invio di missive;
- il sistema di posta elettronica interaziendale non è uno strumento sicuro per la trasmissione di dati appartenenti a particolari categorie (in particolare informazioni sanitarie);
- l'iscrizione a mailing list o newsletter esterne con l'indirizzo aziendale è ammessa esclusivamente per motivi professionali. Prima di iscriversi occorre verificare anticipatamente l'affidabilità del sito che offre servizi;
- in relazione ai contenuti delle comunicazioni e alle modalità di invio occorre adottare tutte le possibili precauzioni anche nell'utilizzo delle e-mail istituzionali, tra cui:
    - eliminare qualunque riferimento a dati personali immediatamente identificativi di un interessato nell'oggetto e nel corpo testo delle comunicazioni di posta elettronica;
    - se risulta necessario inviare la medesima e-mail a più destinatari: inviare una e-mail separata a ciascun interessato o utilizzare lo strumento del Copia Conoscenza Nascosta (CCN) che impedisce ai singoli destinatari la conoscenza diretta degli indirizzi di posta elettronica altrui. L'invio di un singolo messaggio di posta elettronica in copia a destinatari multipli, con gli indirizzi e-mail inseriti in chiaro nel campo di copia conoscenza (CC) o nel campo destinatario (A), può essere effettuato solo se il testo della e-mail è privo di dati personali o appartenenti a categorie particolari (c.d. dati sensibili) di dati e il testo della e-mail risulti di natura generica (es. avvisi, comunicazioni di servizio, note circolari, comunicazioni di chiusure o sospensioni temporanee di attività ecc.) o quando, per mezzo di delibere o altri atti specifici, siano resi pubblici dati personali di dipendenti o collaboratori (nei casi previsti dalla normativa es. delibera aziendale di nomina a Direttore di U.O.);
    - l'inoltro o il re-invio di messaggi di posta elettronica deve essere indirizzato alle sole persone interessate verificando che siano riportati i soli dati necessari alla comunicazione stessa, ivi compresa, nel caso di inoltro di una cronologia di messaggi, la limitazione alla sola sezione di testo che risulti rilevante per l'oggetto della e-mail stessa ed escludendo, quando non strettamente necessaria, la copia integrale di intere conversazioni e-mail;
    - la trasmissione di allegati che possano presentare criticità sotto il profilo della protezione dei dati personali deve essere associata a forme di sicurezza che preservino l'integrità e riservatezza della comunicazione, per esempio con l'uso di archivi;
    - prima della trasmissione di messaggi di posta elettronica è comunque indispensabile accertarsi della digitazione del corretto indirizzo del destinatario, preferendo l'invio tramite Personal Computer a quello effettuato utilizzando

scanner e fotocopiatrici in rete che spesso non consentono l'identificazione del mittente e che espongono a maggiori rischi nella selezione del destinatario. L'utilizzo di tali strumenti condivisi deve quindi essere limitato a casi specifici e solo quando indispensabile (es. invio di scansioni di documenti non altrimenti inoltrabili…).

Nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati personali o dati personali sensibili, è obbligatorio che questi allegati vengano preventivamente resi inintelligibili attraverso crittazione con apposito software (archiviazione e compressione con password). La password di crittazione non deve essere comunicata al destinatario assieme ai dati criptati. Tutte le informazioni, i dati personali e/o sensibili di competenza le possono essere inviati soltanto a destinatari - persone o Enti - qualificati e competenti.

È obbligatorio porre la massima attenzione nell'aprire i file allegati ai messaggi di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti). Al fine di ribadire agli interlocutori la natura esclusivamente aziendale della casella di posta elettronica, i messaggi dovranno contenere una proposizione che descriva l'appartenenza del mittente all'azienda sanitaria (c.d. Firma).

Tutta la posta in transito sul sistema aziendale viene controllata da un sistema antivirus che, oltre a bloccare le e-mail infettate da virus, effettua controlli e seguenti azioni:

- blocco degli allegati potenzialmente pericolosi e pesanti come, per esempio, file eseguibili, filmati audio e file database;
- trasformazione dei link URL contenuti nelle mail, per permettere un controllo preliminare degli stessi durante l'apertura; non è pertanto garantito il funzionamento di questi link URL in caso di re-inoltro all'esterno delle aziende;
- blocco delle e-mail con dimensioni complessive (messaggio di posta e allegati) superiore al limite;
- blocco delle e-mail con numero elevato di destinatari.

In particolari situazioni, ad esempio massicce ricezioni di e-mail infette, il SITI si riserva di bloccare e cancellare (mediante sistemi automatici) le e-mail che contengano particolari allegati o che abbiano nell'oggetto o nel corpo del messaggio particolari parole e/o frasi riconducibili alla violazione di sicurezza o a codice pericoloso.

È fatto obbligo rimanere sotto la propria quota assegnata di spazio, cancellando i messaggi non più utili, sia dalla cartella "Posta in Arrivo" (Inbox) che dalla "Posta inviata" (Sent Items) che dal Cestino (Deleted Items) mantenendo i messaggi nella mailbox al numero minimo. Si ricorda a tal riguardo che le lettere protocollate sono presenti ed accessibili nel sistema informatico del protocollo e che la mailbox non è uno strumento di archiviazione.

Al fine di garantire il corretto funzionamento della posta elettronica aziendale e di evitare la proliferazione del traffico indebito – che in gergo tecnico viene chiamato SPAM – le aziende hanno in uso un sistema AntiSPAM che filtra tutta la posta gestita. Il sistema AntiSPAM utilizza regole euristiche per decidere l'inoltro o meno di un messaggio. Il sistema AntiSPAM analizza il contenuto delle mail in ingresso, inserendo la dicitura "SPAM" all'inizio dell'oggetto qualora il sistema non sia in grado di catalogare chiaramente la mail come SPAM o come regolare. Le regole di filtraggio possono causare il mancato inoltro di posta elettronica erroneamente giudicata dal sistema come SPAM ed al contempo tali regole possono consentire il passaggio di SPAM qualora non siano sufficientemente selettive.

Anche per le ragioni sopra indicate si vieta l'utilizzo della posta elettronica per l'invio di materiali in copie uniche o comunque per l'invio di comunicazioni di cui debba essere garantito l'inoltro al destinatario.
Al fine di aumentare il livello di consapevolezza su un utilizzo sicuro delle risorse, le aziende si riservano l'opportunità di effettuare campagne periodiche per la simulazione di mail phishing, trattando i dati degli utenti per scopi formativi/informativi.
Valgono inoltre i seguenti punti.

- le aziende non assegnano indirizzi di posta elettronica aziendali per usi di tipo personale;
- le aziende non assegnano indirizzi di posta elettronica aziendale a consulenti, ditte manutentrici, liberi professionisti con incarichi terzi eccetera ma esclusivamente a personale trattato nel Sistema Informativo delle Risorse Umane (nei precitati punti 1, 2, 3).;
- le aziende mettono a disposizione funzionalità di avviso in caso di assenza prolungata dell'operatore, che sfruttano le peculiarità del sistema di posta elettronica e possono fornire coordinate di altri riferimenti all'interno dell'azienda tali da garantire il corretto funzionamento dei servizi. L'attivazione di tali misure sarà a cura dell'utente che dovrà attuarla in autonomia;
- ogni assegnatario di indirizzo di posta elettronica aziendale potrà, in caso di necessità, utilizzare un messaggio che menzioni chi all'interno delle aziende assumerà le mansioni durante l'assenza;
- qualora vengano inviati messaggi di posta elettronica che prevedano che l'eventuale risposta possa essere conosciuta da più persone nell'ambito dell'azienda, occorrerà rendere edotto di ciò il destinatario;
- fatte salve le limitazioni di cui ai punti precedenti le aziende favoriscono l'utilizzo della posta elettronica come strumento per la rapida comunicazione fra i dipendenti, fra dipendenti e cittadini, fra pubbliche amministrazioni, purché queste comunicazioni siano parte delle attività istituzionalmente previste e compatibili con le mansioni proprie di ogni operatore.

A titolo di esempio, senza che questo costituisca un elenco esaustivo, tramite la mail non è consentito:

- utilizzare tecniche di "mail spamming" cioè di invio massiccio di comunicazioni non istituzionali o azioni equivalenti;
- utilizzare il servizio di posta elettronica per inoltrare "catene", giochi, scherzi, barzellette e altre e-mail avulse dal contesto lavorativo;
- usare la rete in modo difforme da quanto previsto dal presente documento e dalle leggi penali, civili e amministrative in materia di disciplina dell'attività e dei servizi svolti sulla rete;
- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es.mp3) non legati all'attività lavorativa;
- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list non istituzionali.

Lo strumento di posta elettronica affianca, alle sue funzionalità di office automation altri strumenti integrati tra cui:

- un calendario, utilizzabile per individuare appuntamenti, scadenze o riferimenti correlati alla prestazione lavorativa nonché per organizzare incontri e riunioni allargate. Il calendario personale è condivisibile con altri utenti aziendali secondo livelli differenziati, al fine di consentire un'efficace gestione del lavoro condiviso.
- Un sistema di instant messaging per l'invio di comunicazioni sintetiche.
- Un sistema di videoconferenze per i partecipanti alle riunioni messe a calendario o per chi sta comunicando con il sistema di instant messaging.

4.3. Uso delle liste di distribuzione

Le aziende favoriscono la condivisione di indirizzi di posta elettronica fra più utilizzatori mediante l'adozione di cosiddette "distribution list", cioè di gruppi di indirizzi; una lista di distribuzione altro non è che un indirizzo di posta elettronica al quale viene associato un elenco di altri indirizzi. Non a caso, molto spesso ci si riferisce ad una lista come ad un indirizzario. Il regolamento, per quanto attiene alle liste di distribuzione, comprende inoltre i seguenti punti:

- quando un messaggio di posta elettronica viene inviato ad una lista di distribuzione si ottiene come risultato la ricezione contemporanea dell'e-mail da parte di tutti gli indirizzi che sono compresi in quella lista. Non sono conservate tuttavia le funzionalità di notifiche di ricezione / lettura;
- le liste vengono create, attivate e disattivate dal SITI sulla base delle esigenze degli utenti che tramite la relativa modulistica indicano il gestore della lista stessa
- la creazione avviene dando un nome alla lista, nella forma di un indirizzo di e-mail del tipo: nome-lista@ao.pr.it, nome-lista@ausl.pr.it
- le liste per la distribuzione di comunicazioni mediante posta elettronica aventi come destinatari dipendenti e collaboratori delle azienda, sono predisposte dal SITI e concesse in uso al personale secondo precisi criteri e per scopi specificamente individuati dal delegato;
- le liste di distribuzione costituiscono uno strumento volto ad agevolare lo scambio di informazioni tra i dipendenti ed i collaboratori delle aziende nello svolgimento delle attività professionali o tra i cittadini e l'azienda; il loro utilizzo deve essere finalizzato esclusivamente all'espletamento delle funzioni istituzionali proprie dell'Azienda;
- il servizio di mailing list permette l'invio di comunicazioni elettroniche a determinate categorie di soggetti in relazione alla specifica tipologia di lista utilizzata, nel rispetto della normativa vigente e dei principi generali sopra enunciati, nonché in relazione alle finalità che si intendono perseguire;
- non possono essere inviate mediante le liste di distribuzione aziendali comunicazioni contrarie alla legge, che possano comunque recare danno o pregiudizio all'Azienda o a terzi. A titolo esemplificativo, le liste aziendali non possono essere utilizzate per inviare, anche tramite collegamenti o allegati in qualsiasi formato, messaggi che contengano o rimandino a:
  - pubblicità manifesta o occulta;
  - materiale inviato all'interno delle campagne elettorali
  - comunicazioni commerciali private;
  - materiale discriminante o lesivo della dignità altrui;
  - materiale che violi la normativa a tutela della privacy;
  - contenuti o materiali che violino i diritti di proprietà di terzi;

- altri contenuti contrari o non conformi alla legge e alle attività istituzionali dell'utente.

Il servizio prevede due figure di utilizzatori:

- gli *appartenenti* alla lista, ovvero coloro i cui indirizzi di posta sono inseriti nella lista e che ricevono i messaggi di posta elettronica indirizzate alla lista di distribuzione;
- il *gestore/gestori* della lista: è colui che ne richiede l'utilizzo al SITI (attraverso l'apposita modulistica) e che ne detiene anche il controllo avendo la possibilità di inserire e rimuovere gli appartenenti ed il ruolo associato.

4.4. Creazione e pubblicazione sezioni intranet

L'intranet aziendale costituisce lo strumento principale della rapida condivisione delle informazioni all'interno dell'azienda. La pubblicazione dei contenuti nella homepage della stessa avviene da parte degli uffici comunicazione. È inoltre possibile per alcune articolazioni aziendali disporre di un proprio spazio per la condivisione dei contenuti, condividendone l'opportunità con gli uffici stampa aziendali.

- Ogni sezione intranet ha un suo responsabile, ovvero colui che deve controllare le informazioni pubblicate e la loro correttezza, inoltre è la persona che gestisce l'elenco degli editor (redattori) per la sua sezione.
- Ogni redattore ha tecnicamente la possibilità di modificare qualsiasi articolo presente sulla intranet ma è tenuto a trattare solo gli articoli della propria sezione.
- La pubblicazione delle notizie nella homepage della intranet è in uso esclusivo agli uffici comunicazione.
- È consentito soltanto l'utilizzo di alcuni formati di documenti e immagini, con un limite alla dimensione. Inoltre si specifica che gli articoli pubblicati non possono contenere dati dinamici letti, ad esempio, da database.

4.5. Cartella personale

Il servizio, che viene attivato dopo richiesta del delegato al SITI, permette di usufruire di uno spazio che costituisce una estensione della propria stazione di lavoro; gli utenti accedono alla cartella personale in modalità remota. L'utilizzo è regolamentato dai seguenti punti:

- L'utente è tenuto ad utilizzare la cartella personale per memorizzare informazioni strettamente istituzionali; non può pertanto collocare, anche temporaneamente, in queste aree qualsiasi file che non sia attinente allo svolgimento dell'attività lavorativa. è ' altamente consigliata la periodica (almeno ogni 3 mesi) pulizia di tutti gli spazi assegnati, con cancellazione dei files obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione, salvo casi eccezionali, dei dati al fine di evitare un'archiviazione superflua.
- L'utilizzo della cartella personale è riservato esclusivamente ai compiti di natura strettamente istituzionale, Gli utenti che accedono alla cartella personale devono assicurarsi che i contenuti da loro memorizzati in essa siano esenti da virus, malware o altro tipo di minaccia per la sicurezza del sistema (ad esempio utilizzando sistemi quali antivirus prima di memorizzare dati nella cartella personale). È inoltre fatto esplicito divieto di utilizzare la cartella personale come deposito per software non aziendali o

sprovvisti di idonea e legale licenza d'uso; si evidenzia come i programmi scaricati in versione trial devono sempre essere rimossi terminato il periodo di prova.

- La quantità di dati che un utente può memorizzare sulla cartella personale e/o sull'eventuale cartella condivisa, è limitata (c.d. quota).
- Il personale del SITI nominato amministratore di sistema può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema informatico interaziendale .
- il sistema delle cartelle personali non è volto alla memorizzazione di dati personali e/o particolari in chiaro. In particolari è importante ribadire come il sistema delle cartelle personali non deve essere utilizzato come archivio di referti o documenti sanitari. Per la memorizzazione, esclusivamente transitoria, di documenti contenenti dati personali e/o particolari è necessario l'uso che questi archivi vengano preventivamente resi inintelligibili attraverso crittazione con apposito software (archiviazione e compressione con password). La password di crittazione non deve essere memorizzata assieme ai dati criptati.

4.6. Cartella condivisa

L'azienda favorisce l'uso di cartelle condivise al fine di consentire l'accesso a dati comuni a più utenti che possono usufruire, in tal modo, di uno spazio condiviso sui server centrali. Le cartelle condivise consentono di raccogliere, organizzare e condividere informazioni con altri utenti all'interno dell'azienda. Queste cartelle sono in genere utilizzate da team di progetto o gruppi di utenti per condividere informazioni relative a un settore di interesse comune. Il servizio è regolamentato dai seguenti punti:

- Nella modulistica inviata al SITI è necessario individuare il gestore della cartella e gli utenti che possono avere accesso ai dati contenuti nella cartella. Il gestore ha tutti i permessi di lettura, scrittura e modifica dei dati (intesa come creazione di nuovi dati e cancellazione di tutti i dati presenti). Inoltre può eliminare, aggiungere utenti alla lista degli aventi permesso, con relativa profilatura dei permessi, e modificare i permessi già associati.
- Il gestore deve dare i permessi specifici (lettura, scrittura, modifica) a seconda delle esigenze del servizio. L'utente è tenuto ad utilizzare le unità di rete per la condivisione di informazioni strettamente istituzionali; non può pertanto collocare, anche temporaneamente, in queste aree, qualsiasi file che non sia attinente allo svolgimento dell'attività lavorativa. è altamente consigliata la periodica (almeno ogni 3 mesi) pulizia di tutti gli spazi assegnati, con cancellazione dei files obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione, salvo casi eccezionali, dei dati al fine di evitare un'archiviazione superflua. Nel caso si renda necessario, in conformità ai principi del GDPR (tra cui in particolare la minimizzazione), mantenere dei dati ivi presenti sarà necessario adottare tecniche di backup per l'accesso asincrono ai dati stesso (ad esempio con un backup su DVD gestito con modalità sicure) previa autorizzazione del delegato al trattamento).
- Gli utenti che accedono alla cartella condivisa devono assicurarsi che i contenuti memorizzati in essa siano esenti da virus, malware o altro tipo di minaccia per la sicurezza del sistema. Lo spazio disponibile non viene calcolato sulla cartella, ma su ogni utente. Ogni utente può memorizzare sul server dove risiede la cartella i propri file che

concorrono a raggiungere il limite del punto precedente. Questa è la quota personale totale a disposizione e può essere distribuita su più cartelle. Una volta raggiunto il limite personale, il sistema non permetterà più la memorizzazione di ulteriori dati. Si raccomanda lo spostamento dei dati meno recenti su supporti esterni valutandone l'appropriata modalità di conservazione.

- Le cartelle condivise presenti nei server sono aree di condivisione di informazioni strettamente istituzionali e non possono in alcun modo essere utilizzate per scopi diversi.
- Su queste unità vengono svolte regolari attività di amministrazione e backup da parte del personale del SITI. Si ricorda che tutti i dischi o altre unità di memorizzazione locali (es. disco C: interno al PC) non sono soggette a salvataggio da parte del personale incaricato del SITI. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente. Non costituisce pratica sicura di memorizzazione salvare informazioni e dati personali su PC aziendali nello spazio locale (es. su desktop; nella cartella documenti…). L'utente è tenuto a utilizzare la cartella che risiede sul server aziendale per la memorizzazione di informazioni e dati strettamente necessari all'attività istituzionale.
- Il personale del SITI può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema informatico aziendale sia sui PC degli utenti sia sulle cartelle condivise.
- il sistema delle cartelle convidivse non è volto alla memorizzazione di dati personali e/o particolari in chiaro. In particolari è importante ribadire come il sistema delle cartelle personali non deve essere utilizzato come archivio di referti o documenti sanitari. Per la memorizzazione, esclusivamente transitoria, di documenti contenenti dati personali e/o particolari è necessario l'uso che questi archivi vengano preventivamente resi inintelligibili attraverso crittazione con apposito software (archiviazione e compressione con password). La password di crittazione non deve essere memorizzata assieme ai dati criptati.

In caso di prolungata assenza di un incaricato che impedisce l'accesso ai files conservati nelle cartelle condivise si distinguono due diversi casi:

1. i dati siano accessibili da più operatori;
2. i dati siano accessibili da parte di un unico operatore.

Qualora i dati siano accessibili da parte di più operatori – caso 1 - sarà necessario adottare le misure di seguito descritte solo nell'ipotesi in cui tutti gli operatori che hanno accesso ad un medesimo file non siano presenti per un lungo periodo; tale casistica di seguito per semplicità si farà riferimento al solo punto 2:

- nel caso il delegato al trattamento non sia in grado di accedere direttamente ai files giacenti nella cartella condivisa, farà richiesta al gestore degli accessi di tale cartella nel caso in cui anche il gestore della cartella non possa per lungo periodo gestire gli accessi, sarà cura del delegato del trattamento potrà riassegnare il ruolo di gestore cartella tramite modulistica);
- nel caso il delegato del trattamento sia in grado di utilizzare gli strumenti informatici normalmente utilizzati dall'operatore, basterà che il delegato al trattamento acceda ai file al posto dell'operatore assente. Si raccomanda che delegato del trattamento informi di ciò gli incaricati assenti alla prima occasione utile.

4.7. Posta elettronica certificata

Le aziende promuovono l'uso della Posta elettronica certificata per lo scambio di documentazione tra pubbliche amministrazioni e tra pubblica amministrazione e cittadini.
In tal senso sono istituiti gli indirizzi PEC dei servizi centrali alle direzioni delle aziende. Per le strutture organizzative non afferenti alle direzioni è facoltà dei Direttori di struttura complessa o semplice dipartimentale richiedere l'istituzione tramite le procedure di richiesta attivazioni del SITI.
L'attribuzione dell'indirizzo PEC sarà sempre nominale ed associato al Direttore della struttura di riferimento che ha il compito, in caso di cessazione dell'incarico di direzione della struttura, di passare le consegne sulla corretta gestione dell'indirizzo PEC.
La disattivazione degli indirizzi PEC avviene esclusivamente su richiesta del precitato Direttore o di persona a lui sovraordinata.

5. Utilizzo delle attrezzature informatiche

5.1. Utilizzo delle Postazioni di Lavoro informatizzate

Le postazioni di lavoro informatizzate (quali Personal Computer, totem informativi eccetera) sono affidate al responsabile di struttura e rappresentano un strumento di lavoro. Ogni postazione di lavoro informatizzata è in carico ad uno specifico centro di costo e la corretta gestione e tenuta della postazione di lavoro informatizzata fa capo al responsabile del centro di costo.
Ogni utilizzo della postazione di lavoro informatizzata non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. La postazione di lavoro informatizzata deve essere custodita con cura evitando ogni possibile forma di danneggiamento.
Rientrano nella corretta custodia: l'alimentazione tramite prese dedicate; il posizionamento sopraelevato e lontano da zone polverose e la rimozione di eventuali elementi ostruenti dalle prese di raffreddamento.
La richiesta di postazioni informatiche rientra nei normali percorsi di richiesta di nuove attrezzature (es. budget). La richiesta, oltre che sotto il profilo economico, sarà valutata anche dal punto di vista tecnico dal SITI che verificherà la correlazione tra il numero di postazioni informatiche, la destinazione d'uso dei locali ed il posizionamento fisico nei locali individuati (atto a supportare il rispetto del Dlgs 81/2008 da parte del dirigente della sicurezza relativo ai locali di installazione).
La postazione di lavoro informatizzata data in affidamento all'utente permette l'accesso ai sistemi interaziendali solo attraverso specifiche credenziali di autenticazione come già descritto.
Il personale incaricato che opera presso il SITI (o eventuali ditte fornitrici) è 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 eccetera).
Detti interventi, potranno anche comportare l'accesso in qualunque momento, ai dati trattati da ciascuno. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività delle aziende, si applica anche in caso di assenza prolungata od impedimento dell'utente.
Il personale incaricato del SITI (o di eventuali ditte fornitrici) ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni al fine di garantire l'assistenza tecnica

e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware eccetera. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.
Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale del SITI né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre Virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone le aziende a gravi rischi; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software, che impone la presenza nel sistema di software regolarmente licenziato, vengono sanzionate anche penalmente. Si ricorda che tali violazioni sono totalmente imputabili all'utente che ha installato i suddetti software e sollevano le aziende da qualsivoglia responsabilità.
Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, chiavette internet)
Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, richiedendo una verifica manutentiva, tramite l'apposita richiesta di intervento manutentivo SITI, nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo punto del presente Regolamento relativo alle procedure di protezione antivirus.
La postazione di lavoro informatizzata deve essere spenta prima di lasciare gli uffici, in caso di suo inutilizzo o in caso di assenze prolungate dall'ufficio, a meno di utilizzo remoto da altre sedi. Si ricorda che lasciare un elaboratore incustodito e con l'apposita funzione di blocca schermo disabilitata, può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.
Al fine di tutelare la continuità operativa del sistema informatico aziendale si ricorda che il SITI può provvedere senza preavviso (ad esempio in caso di emergenze quali attacchi informatico o infezioni vitali) all'aggiornamento software di tutte le postazioni anche se questo prevede un immediato riavvio dell'elaboratore.
In generale si ricorda che, nel contesto del sistema informatico, la disponibilità di una determinata funzionalità non autorizza il consegnatario di un bene all'utilizzo della stessa se non espressamente autorizzato e comunque se non necessario all'espletamento delle proprie mansioni e riconducibile ad attività istituzionali.
A tal riguardo è bene precisare che talvolta non è possibile disabilitare determinate funzionalità da alcuni apparati tecnologici quali le postazioni di lavoro informatizzate, o che questo, anche se tecnicamente possibile, può rappresentare un onere sproporzionato per l'azienda così come espresso nell'art 32 del GDPR.
Le AASS si riservano di verificare, anche tramite il SITI, l'utilizzo pertinente degli strumenti informatici concessi in uso – ad esempio le stazioni di lavoro informatizzate, i palmari eccetera. qualora si evidenzino volumi anomali di traffico o vi siano altri elementi che indichino un uso non conforme alle presenti indicazioni.
Le verifiche avverranno in modo graduale nel rispetto della normativa vigente. Le aziende si riservano inoltre, anche tramite il SITI ed in casi di estrema gravità, di disconnettere forzatamente la postazione informatica qualora questa metta a repentaglio la funzionalità e la sicurezza del resto della rete informatica.

Le AASS vietano la memorizzazione e/o il trattamento di dati di qualsiasi tipo a fini personali per mezzo o all'interno delle postazioni di lavoro informatizzate concesse in uso. Il SITI (tramite personale proprio o ditte manutentrici) può accedere a detti strumenti per compiti connessi alla rispettiva funzione e mansione. Non potrà essere addotto, come impedimento all'accesso, il fatto che siano presenti dati utilizzati a fini personali, in forza del suddetto divieto di gestire dati non connessi alla propria mansione e/o attività istituzionali.
Si raccomanda di utilizzare la massima attenzione nell'utilizzo delle macchine fotocopiatrici di ultima generazione che possono scansionare e memorizzare documenti, talvolta conservando il file elettronico al proprio interno.
In caso di stampa o duplicazione non riuscite in cartaceo di documentazione contenente dati personali / sensibili occorre rendere illeggibile il contenuto dei dati (es. tritura del materiale cartaceo).
Gli utenti in caso di assenza, anche momentanea, dalla propria postazione di lavoro, devono adottare tutte le misure atte ad escludere che soggetti non autorizzati possano acquisire la conoscenza di informazioni riservate o accedere alle banche dati; ad esempio disconnettendosi, bloccando la postazione di lavoro o attivando un salvaschermo protetto da password.

E' facoltà esclusiva del SITI (tramite personale proprio e/o ditte manutentrici) installare nuovi software sulle postazioni utente.
Ogni utente è responsabile dell'utilizzo dei sistemi software in modo corretto sulle postazioni aziendali. In particolare è responsabilità dell'utente il rispetto delle normative relative al software (es. uso software protetto da Copyright senza l'acquisto delle regolari licenze) sul computer che gli è affidato.
E' vietato diffondere software soggetto a Copyright acquistato dalle aziende, al di fuori dei termini delle licenze.
E' vietato diffondere software che possa danneggiare le risorse informatiche, anche via e-mail.
E' vietato accedere a dati e/o programmi per i quali non si ha esplicita autorizzazione o incarico e se non necessario per l'espletamento dell'attività istituzionale.
Il SITI (tramite personale proprio o ditte manutentrici) può accedere ai sistemi informatici per manutenzione preventiva e correttiva. L'accesso potrà avvenire, anche senza preavviso in casi di evidente emergenza/urgenza organizzativa (diffusione virale, aggiornamento massivo) o su specifica richiesta dell'autorità giudiziaria.
Si ricorda infine che è vietato manomettere o cambiare le configurazioni delle postazioni informatiche.

5.2. Utilizzo di Notebook

L'utente è responsabile del Notebook (o PC portatile o tablet) assegnatogli dal SITI e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
Se connessi alla rete interaziendale, a tali dispositivi si applicano le regole di utilizzo previste dal presente regolamento, con particolare attenzione alla rimozione di eventuali file elaborati prima della riconsegna.
Questi dispositivi, utilizzati all'esterno delle sedi lavorative, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni. Sarà cura e carico dell'utente dare tempestiva comunicazione al SITI in caso di sottrazione e/o danni apportati alla tecnologia informatica consegnata, nonché eventuali segnalazioni all'autorità giudiziaria in caso di furto. Qualora questi strumenti debbano essere

utilizzati anche tramite reti esterne a quella interaziendale sarà necessario che l'assegnatario presti una maggiore attenzione alla sicurezza. Tali tecnologie saranno quindi inseriti nel dominio aziendale a seconda delle necessità del singolo utente a totale descrizione del SITI.

5.3. Utilizzo e conservazione dei supporti rimovibili

Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB eccetera), se previsto dalle procedure , contenenti dati personali nonché informazioni costituenti know-how aziendale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.
Tutti i supporti magnetici rimovibili devono essere crittografati o contenere file con password in modo che l'eventuale perdita o sottrazione non consenta a terzi non autorizzati alla visione del suo contenuto.
Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati personali, ciascun utente dovrà utilizzare un apposito strumento software (reperibile nella intranet aziendale).
In ogni caso i supporti magnetici contenenti dati personali devono essere dagli utenti adeguatamente custoditi (es. armadi chiusi); terminatone l'utilizzo i dati in esso contenuti devono essere cancellati in modo irrecuperabile.
L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.
E' vietato l'utilizzo di supporti rimovibili, come ad esempio floppy disk/cd rom o chiavette USB, per lo scambio di dati personali; qualora vi fosse assoluta necessità di utilizzarli è indispensabile assicurarsi che essi non vengano riutilizzati e siano distrutti dopo il loro utilizzo; qualora, viceversa, vengano riutilizzati occorre verificare che il precedente contenuto sia stato reso assolutamente irrecuperabile.

5.4. Rete attiva di trasmissione dati

La rete Intranet (rete dati attiva di trasmissione interna) è un bene aziendale destinato a supportare lo svolgimento dei compiti istituzionali attraverso il sistema informatico aziendale. È vietata qualsiasi azione atta a degradare il sistema. A titolo esemplificativo valgono i seguenti punti volti a mantenere il corretto livello di sicurezza della rete di trasmissione dati.

- È fatto esplicito divieto di inserimento nella rete (wired o wireless) delle aziende di postazioni informatiche personali/non aziendali.
- È vietato installare sulle reti aziendali apparecchiature/attrezzature di rete (quali Switch, Hub, Access point eccetera) non preventivamente autorizzate dal SITI. Si precisa inoltre che su tali apparecchiature è fatto divieto assoluto di qualsivoglia intervento (compresa l'aggiunta di ulteriori postazioni informatiche) eccezione fatta per i manutentori afferenti ai servizi tecnici interaziendali;
- Aziende ed enti esterni possono collegare in rete loro apparati o sistemi soltanto se legati alle aziende da convenzione o contratto di fornitura. Tali apparati dovranno comunque rispettare in pieno i dettami del presente regolamento ed inoltre il responsabile unico del procedimento/direttore dell'esecuzione sarà responsabile sulla vigilanza del rispetto del regolamento da parte di tale azienda/ente. Il responsabile unico del procedimento/direttore dell'esecuzione, persona fisica dipendente di una delle due aziende, sarà inoltre responsabile di atti diretti o indiretti relativi al sistema informatico effettuati tramite tali apparati/sistemi. Resta inteso che il posizionamento di apparati sulla rete aziendale avverrà secondo le indicazioni del SITI. A titolo esemplificativo si riporta:

- Il divieto di configurare servizi di rete centralizzati, quali DNS, DHCP, mailing, Web Server, accesso remoto (dial-up);
- È consentito installare apparati wireless (access point, bridge, repetear eccetera) esclusivamente se questi non recano alcuna sovrapposizione / interferenza con i sistemi wireless manutenuti dal SITI; tali installazioni possono essere effettuate esclusivamente dai servizi tecnici interaziendali;
- E' vietato intercettare/monitorare/ascoltare/leggere comunicazioni sulla rete di trasmissione dati e utilizzare strumenti atti a raccogliere queste informazioni.

- Il solo personale addetto alla manutenzione, al controllo e alla sicurezza delle infrastrutture tecnologiche è autorizzato a compiere le attività che garantiscano oltre il buon funzionamento delle infrastrutture aziendali anche il perseguimento dei fini istituzionali nei limiti e nel rispetto della normativa vigente.

5.5. Strumenti informatici di supporto

Il sistema informatico è composto da strumenti periferici correlati alle postazioni informatiche e/o agli applicativi (es. rilevatori presenze, lettori di barcode, stampanti di braccialetto, lettori di schede ottiche...). Non rientrano in questa categoria gli strumenti hardware (c.d. attrezzature sanitarie) correlati con l'attività clinica per diagnosi, prevenzione, controllo, terapia o attenuazione di una malattia.
Gli strumenti informatici di supporto trattano dati correlati all'organizzazione ed ai compiti istituzionali delle due aziende e, in modo simile a quanto indicato per le postazioni informatiche e la rete attiva di trasmissione dati, è vietata qualsiasi azione atta a degradare il sistema informatico e/o supporti informatici.
A titolo esemplificativo valgono i seguenti punti atti a mantenere il corretto livello di sicurezza del sistema informatico:

- È fatto esplicito divieto di connettere/disconnettere o riconfigurare gli strumenti informatici di supporto eccezione fatta per i manutentori afferenti al SITI.
- È fatto altrettanto divieto di spostare gli strumenti informatici di supporto da una postazione informatica ad un'altra (es. scambio stampante da postazioni informatiche) eccezione fatta per i manutentori afferenti al SITI.
- È vietato installare sulle postazioni informatiche strumenti informatici di supporto eccezione fatta per i manutentori afferenti al SITI.
- Aziende ed enti esterni possono collegare in rete loro strumenti informatici di supporto soltanto se legati all'Azienda da convenzione o contratto di fornitura. Tali apparati dovranno comunque rispettare in pieno i dettami del presente regolamento ed inoltre il responsabile unico del procedimento/direttore dell'esecuzione sarà responsabile sulla vigilanza del rispetto del regolamento da parte di tale ente. Il responsabile unico del procedimento/direttore dell'esecuzione, persona fisica dipendente di una delle due aziende, sarà inoltre responsabile di atti diretti o indiretti relativi al sistema informatico effettuati tramite tali apparati/sistemi. Resta inteso che il posizionamento di strumenti informatici di supporto con il resto del sistema informatico avverrà secondo le indicazioni del SITI.
- E' vietato intercettare/monitorare/ascoltare/leggere comunicazioni sugli strumenti informatici di supporto e utilizzare strumenti atti a raccogliere queste informazioni.

Il solo personale addetto alla manutenzione, al controllo e alla sicurezza delle infrastrutture tecnologiche è autorizzato a compiere le attività che garantiscano oltre il buon funzionamento delle infrastrutture aziendali anche il perseguimento dei fini istituzionali nei limiti e nel rispetto della normativa vigente.
Si ritiene importante ricordare che il corretto caricamento/sostituzione del materiale di consumo non rientra tra le operazioni manutentive ma che è di competenza dell'utilizzatore finale (es. sostituzione toner e drum).

5.6. Misure di sicurezza e Piano ICT

Il sistema informatico interaziendale è oggetto di continuo intervento per la salvaguardia della sicurezza dello stesso. In particolare sono perseguite la misure di sicurezza AGID tra cui, sono richiamati di seguito, alcuni dei principali elementi di riflesso sull'utente del sistema informatico interaziendale.
Il sistema informatico interaziendale è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico interaziendale mediante virus o mediante ogni altro software aggressivo. Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso **senza spegnere il computer** nonché segnalare prontamente l'accaduto al personale del SITI; in particolare l'utente dovrà comunque porre la massima attenzione nell'aprire i file allegati di posta elettronica prima del loro utilizzo, analizzando l'attendibilità del mittente, la correttezza dell'oggetto della mail ed il nome del file allegato che si è invitati ad aprire. Ogni dispositivo di archiviazione di provenienza esterna alle aziende dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale del SITI e non utilizzato.
L'aggiornamento delle misure di sicurezza AGID, delle tecnologie oggetto di questo regolamento, è una delle attività strategiche condotte dai SITI (si veda a tal riguardo l'apposita procedura di gestione delle attività). Annualmente viene prodotto, da parte del Responsabile della Transizione Digitale, un documento che riporta al Titolare lo stato dell'arte dell'adozione delle misure di sicurezza AGID.
Le misure di sicurezza AGID si inseriscono nel più generale ambito del perseguimento del Piano ICT interaziendale che, discendendo dal Piano AGID nazionale, declina a livello locale gli obbiettivi e le attività che costituiscono obblighi normativi relativi al mondo ICT. Al pari delle misure di sicurezza il perseguimento del Piano ICT è un aspetto fondamentale per il corretto funzionamento dei sistemi ICT governati dal SITI (anche in questo caso si rimanda ad apposita procedura di aggiornamento delle attività).
Gli amministratori di sistema delle tecnologie oggetto di questo regolamento sono individuati nell'apposito strumento di gestione dei sistemi ICT.

5.7. Tecnologie informatiche personali e accessi da remoto

Le aziende così come previsto nei recenti CCNL e nel Piano Operativo Lavoro Agile, al fine di permettere il c.d. Smartworking, e per permettere a fornitori terzi e/o consulenti l'operatività da

remoto consentono, a determinate condizioni tecnologiche, la connessione di tecnologie informatiche private alla zona protetta di lavoro del sistema informatico interaziendale.
Per il personale afferente alle AASS (vedi paragrafo 4.1) l'accesso avviene tramite VPN via Https (c.d. Smartworking web).
Il collaboratore che si connette al precitato sistema garantisce che:

- la tecnologia informatica personale (es. PC o tablet) risponde in tutto e per tutto alle misure di sicurezza AGID al livello adeguate al trattamento in essere;
- effettuerà stampe locali al proprio PC solo di documenti privi di dati personali;
- non effettuerà esportazioni o salvataggi locali di dati sulla propria postazione personale;

Per il personale afferente ai fornitori terzi (vedi paragrafo 4.1 punti 6 e 7) l'accesso avviene tramite VPN/SSL.
Il consulente che si connette al precitato sistema garantisce che:

- la tecnologia informatica personale (es. PC o tablet) risponde in tutto e per tutto alle misure di sicurezza AGID al livello adeguate al trattamento in essere;
- effettuerà stampe locali al proprio PC solo di documenti privi di dati personali;
- non effettuerà esportazioni o salvataggi locali di dati sulla propria postazione personale; manterrà, sui propri sistemi personali, separati le partizioni dedicate all'attività lavorativa da quelle personali o di altri clienti.

In entrambi i casi l'accesso verrà tecnicamente rilasciato dal SITI previa compilazione della modulistica on line e previa valutazione del delegato richiedente della correttezza normativa dell'accesso che si intende rilasciare (es. normativa su telelavoro e previsioni contrattuali con fornitore terzo).

6. Sistemi software

6.1. Principi base

Il sistema informatico interaziendale è costituito da quattro classi principali di software cui di seguito si fornisce una breve descrizione:

A) sistemi software di base con licenza *open*. Essi sono solitamente installati sulle postazioni client e non costituiscono parte integrante del sistema informativo aziendale; sono gli strumenti software che permettono l'elaborazione di documenti o l'esecuzione di funzionalità di sistema. Rientrano tra questi sistemi i software d'ufficio (editor di testi, foglio di calcolo...), gli elaboratori di immagini, i browser e gli strumenti di compressione e firma digitale, e tutti i software che sono liberamente accessibili dalla rete, cioè che sono distribuiti con licenze *open source* o *public domain* e che pertanto non determinano un costo diretto per l'azienda.
B) Sistemi software di base con licenza commerciale. Questi sistemi sono, dal punto di vista tecnico, del tutto simili ai precedenti. La principale caratteristica di questi sistemi è la licenza con cui sono distribuiti; essa costituisce un costo diretto per l'azienda.
C) Sistemi software applicativi. Questi sistemi sono gli strumenti informatici di gestione del sistema informativo interaziendale. Rientrano tra questi sistemi, ad esempio, gli strumenti di gestione dei ricoveri, di gestione ambulatoriale, del pronto soccorso, dei

laboratori, della manutenzione e del bilancio. I sistemi applicativi trattano, in modo strutturato, dati fondamentali per la gestione aziendale.

D) Sistemi software applicativi terzi. Questi sistemi sono gli strumenti informatici che gestiscono parte del sistema informativo aziendale ma gestiti, manutenuti e resi accessibili da organi terzi rispetto al SITI (i.e. sistemi regionali, sistemi forniti da altri servizi, sistemi ministeriali eccetera).

La diversa modalità di gestione dei quattro sistemi dipende dalla differenza tecnologica, organizzativa e di ruolo che i sistemi hanno tra loro. È importante notare che, a prescindere dai sistemi in esame, è compito del delegato al trattamento dati e dei relativi autorizzati al trattamento ex art. 29 Regolamento (UE) 2016/679 e art. 2 quaterdecies Codice Privacy l'utilizzo dei sistemi software in modo conforme ed in rispetto al corretto trattamento dei dati oltre che della normativa vigente.
In tutte le diverse modalità si evidenzia che il sistema informatico (e quindi anche i software dei punti precedenti) sono un elemento distinto dai dati in esso contenuti. La qualità informativa e la correttezza dei dati (e le conseguenze organizzative derivanti) dipendono dall'attività dei soggetti autorizzati sotto la vigilanza del/dei delegati al trattamento specifici.

6.2. Sistemi software di base con licenza open

La lista dei software di base presenti nelle AASS con licenza open presenti (indicata come tale dalla Open Source Initiative o dalla Free Software Foundation) è a disposizione sulla intranet aziendale nella sezione del SITI.
I sistemi software di base con licenza open sono installabili e rimovibili con una richiesta di intervento manutentivo sul PC gestito dal SITI.
L'inclusione di un software nella lista è a completa discrezione del SITI poiché la compatibilità tra tali sistemi software ed il resto del sistema informatico non è garantita. È possibile farne richiesta tramite apposita modulistica al SITI che valuterà la compatibilità tecnica e l'utilità informativa degli stessi.
L'assistenza e la manutenzione su tali sistemi software non saranno forniti; essi, come recita la licenza d'uso, sono concessi in modalità "AS IS".
La formazione all'uso di tali strumenti potrà essere richiesta all'interno degli appositi percorsi aziendali.

6.3. Sistemi software di base con licenza commerciale

I sistemi software di base con licenza commerciale sono assegnati ad un determinato centro di costo in modo del tutto simile a quanto avviene per le generiche attrezzature (i.e. PC e stampanti).
La richiesta di tali software rientra pertanto nei normali percorsi di richiesta di nuove attrezzature (i.e. budget). La richiesta, oltre che il percorso economico, sarà valutata anche dal punto di vista tecnico dal SITI (i.e. compatibilità tecnica e utilità informativa).
L'assistenza e la manutenzione su tali sistemi software non saranno forniti; essi, come recita la licenza d'uso, sono concessi in modalità "AS IS".
La formazione all'uso di tali strumenti potrà essere richiesta all'interno degli appositi percorsi aziendali.

6.4. Sistemi software applicativi

I sistemi software applicativi sono gli strumenti informatici di gestione del sistema informativo manutenuti dal servizio informativo aziendale. Sono gli strumenti che trattano in modo strutturato i dati di rilievo aziendale e le relative procedure. Rientrano tra questi sistemi, ad esempio, gli strumenti di gestione dei ricoveri, di gestione ambulatoriale, del pronto soccorso, dei laboratori, degli acquisti e del bilancio.
In relazione alla grande importanza che i sistemi software applicativi rivestono all'interno del sistema informatico è bene distinguere le loro modalità di gestione in cinque distinte fasi:

- **Acquisizione**. La richiesta di nuove dotazioni relativi a software applicativi rientrano nei percorsi di richiesta di nuove attrezzature (i.e. percorso di budget, progetto, board degli investimenti). Tali richieste debbono essere accompagnate da:
    - l'individuazione di almeno un referente applicativo all'interno dell'articolazione aziendale che definirà con il SITI le modalità di funzionamento dell'applicativo e le modalità di accesso;
    - l'analisi dei percorsi organizzativi aziendali che il sistema applicativo andrà ad informatizzare (fondamentale per l'informatizzazione risulta la disponibilità di procedure aziendali e/o modulistica);
    - l'analisi del risparmio di materiale e/o personale, del miglioramento della qualità dei processi e di analisi dei rischi;
    - riferimenti normativi, linee guida e/o raccomandazioni.

La richiesta verrà analizzata dal punto di vista tecnico e organizzativo dal SITI e dalle articolazioni aziendali coinvolte nei processi descritti. In caso di esito positivo, lo strumento informatico sarà quindi implementato in accordo alla programmazione aziendale. A tal riguardo, è bene ricordare che il programma di informatizzazione interaziendale è definito sulla base delle linee guida europee sulla sanità elettronica e l'*e-health*, il *piano AGID* ed i piani ICT regionali ed interaziendali.
L'implementazione delle soluzioni software vede l'attiva partecipazione, oltre che del fornitore del sistema software applicativo, del SITI e del referente applicativo; essa termina con un collaudo tecnico/funzionale che prevede la partecipazione di tutte le precitate figure.
Il sistema software applicativo, a seguito del collaudo, (oltre che dal suo normale utilizzo a supporto delle procedure organizzative definite in sede di analisi) è caratterizzato dalle seguenti fasi del proprio ciclo di vita:.

- **Manutenzione correttiva**. L'assistenza e la manutenzione correttiva, dal punto di vista tecnico, del sistema software è coordinata dal SITI (con l'apposita stipula di contratti di manutenzione con i fornitori del sistema). L'orario di copertura del manutentore ed i livelli di servizio sono concordati dal SITI con i/gli referente/i applicativo e in rispondenza alle disponibilità economiche.
- **Manutenzione evolutiva**. L'implementazione di variazioni sugli strumenti informatici è realizzata dal SITI, sulla base della programmazione economica del servizio, attraverso le priorità concordate con i/gli referente/i applicativo e con la programmazione ICT (ministeriale, regionale ed aziendale).
- **Estrazione dati**. L'estrazione di dati dal sistema informatico avviene tramite le funzionalità presenti nello strumento applicativo. Tipologie diverse di estrazioni dati potranno essere richieste dal referente applicativo e, concordemente con la fattibilità tecnica ed economica, verranno realizzate ~~su~~ in seguito alla presentazione di richieste puntuali.

Ogni tipologia di estrazione dati dai sistemi nelle modalità sovraindicate potrà essere utilizzata dai singoli autorizzati e/o delegati se e solo se compatibile con la vigente normativa relativa al trattamento dati (GDPR). È responsabilità dell'utente che estrae tramite le funzionalità applicative disporre delle apposite autorizzazioni in conformità al GDPR. Parimenti le richieste del referente applicativo poste al SITI e volte all'estrazione debbono essere intesi come già valutate ed autorizzate dal delegato di riferimento in conformità al GDPR.

- **Flussi informativi**. La realizzazione di flussi informativi ministeriali o regionali avviene a partire dai sistemi applicativi concordemente con il referente applicativo.
  La realizzazione di flussi informativi ad uso interno è realizzata depositando i dati dei sistemi applicativi nel datawarehouse. Tali realizzazioni potranno essere effettuate su richiesta delle articolazioni interaziendali che accedono al datawarehouse concordemente al referente applicativo dei sistemi applicativi originanti i dati in base alla fattibilità tecnico/economica.

La formazione all'uso di tali strumenti potrà essere richiesta, concordemente con il referente applicativo, all'interno degli appositi percorsi aziendali.

I sistemi software applicativi possono infine terminare il proprio ciclo di vita e non essere più facenti parte del sistema informativo interaziendale. Le motivazioni per cui i sistemi software terminano il proprio ciclo di vita comprendono tematiche tecniche (termine supporto del fornitore, indisponibilità di piattaforme adeguate …) ed organizzative (indisponibilità economiche, variate esigenze organizzative, …). È importante ricordare come il termine del ciclo di vita di un software applicativo può non corrispondere con la sua indisponibilità tecnica; in altre parole un software potrebbe, a seconda della sua posizione tecnologica, continuare ad essere disponibile al termine del suo ciclo di vita (ad esempio per permettere la consultazione di informazioni storiche).

La lista dei sistemi software applicativi presenti nelle aziende, che comprende i correlati referenti applicativi e lo stadio del ciclo di vita del software, è a disposizione sulla intranet aziendale nella sezione del SITI. In particolare si evidenziano i seguenti stadi: *in test* (l'applicazione è in sperimentazione tecnica), pilota (l'applicazione è in sperimentazione funzionale ed il suo utilizzo non è da considerarsi definitivo), attivo (l'applicazione è utilizzabile correntemente), deprecato (l'applicazione è temporaneamente utilizzabile fino a completa dismissione), non attivo (l'applicazione è dismessa, non più utilizzabile).

Tutto il processo di gestione degli strumenti software applicativi è realizzato dal SITI con il supporto della figura del referente applicativo. Risulta quindi importante riassumere le competenze di quest'ultimo:

- La persona è individuata dal SITI, in accordo con i Delegati al trattamento dati gestiti dall'applicativo, tra il personale che afferisce a questi ultimi (autorizzati al trattamento ex art. 29 Regolamento (UE) 2016/679 e art. 2 quaterdecies Codice Privacy). In caso di presenza di più delegati al trattamento dati interessati dal medesimo applicativo è possibile che il SITI individui più referenti applicativi.
- Il referente costituisce il punto di riferimento per gli aspetti organizzativi dell'applicativo, delle modalità di funzionamento dello stesso e delle politiche d'accesso (anche con il supporto del Gruppo Privacy). Il referente partecipa attivamente in collaborazione al SITI alla definizione delle priorità delle modifiche all'applicativo.
- È bene evidenziare che il referente applicativo rappresenta il riferimento per il SITI, per le rispettive competenze, necessario per la corretta conduzione delle modifiche/integrazioni applicative.

Il referente applicativo può talvolta disporre, in luogo della collaborazione diretta con il SITI ed allo scopo di supportare gli utilizzatori del sistema informatico, del sistema di condivisione del desktop normalmente utilizzato dal SITI e di particolari profili ed abilitazioni applicative.

6.5. Sistemi software applicativi terzi

I sistemi software applicativi terzi sono gli strumenti informatici di gestione del sistema informativo forniti da terze parti. Sono gli strumenti che trattano in modo strutturato dati di rilievo ma non gestiti dal SITI. Rientrano tra questi sistemi, ad esempio, gli strumenti di richiesta trasporti su gomma, cartelle informatica del MMG, prenotazioni pasti, centralino telefonico ed il sistema PACS/RIS.
È possibile richiedere al SITI il posizionamento nella intranet del collegamento a tali sistemi software. Tali richieste, come da apposita modulistica, debbono essere accompagnate dall'individuazione di un referente del collegamento all'interno dell'articolazione aziendale oltre che dalle indicazioni relative alla manutenzione ed ai contatti (telefonici e/o email).
L'assistenza e la manutenzione, dal punto di vista tecnico, del sistema software sarà fornita (ove presente) dalle strutture aziendali, interaziendali e/o extra-aziendali correlate. Essa non sarà comunque effettuata dal SITI.
La formazione all'uso di tali strumenti potrà essere richiesta, concordemente con il referente applicativo, all'interno degli appositi percorsi interaziendali.

7. Conclusione

Ogni utente è personalmente responsabile dell'utilizzo dei beni e delle risorse informatiche affidatigli dalle AASS, nonché dei relativi dati trattati per finalità aziendali .

7.1. Garanzie fornite dalle aziende

Alla luce dell'art. 4, comma 1, l. n. 300/1970, la disciplina della materia indicata nel presente Regolamento, non è finalizzata all'esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro ma solo a permettere a quest'ultimo di utilizzare i sistemi informatici per fare fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali
Le AASS tutelano gli utenti del sistema informatico e rendono possibile l'accesso a log o altre registrazioni tecniche ai fini di controlli interni tecnici o su richiesta dell'autorità giudiziaria. Eventuali altre richieste ad accessi a log o altre registrazioni tecniche realizzabili tramite il sistema informatico aziendale saranno realizzate previa valutazione all'interno del Gruppo Privacy.

7.2. Controlli

Le AASS, per esigenze organizzative, produttive, di sicurezza e di tutela del patrimonio, si riservano di effettuare controlli sul corretto utilizzo di internet, della posta elettronica, delle apparecchiature informatiche e di tutti i sistemi ICT nel rispetto delle normative vigenti e del presente regolamento.
Qualora, durante tali controlli, vengano rilevate anomalie nell'utilizzo degli strumenti informatici, il SITI procede preliminarmente all'invio di un avviso generalizzato relativo all'uso improprio riscontrato, con l'invito ad attenersi scrupolosamente al presente regolamento, e riservandosi la facoltà di svolgere successive azioni mirate alla verifica del corretto utilizzo. I controlli posti in

essere saranno sempre tali da evitare ingiustificate interferenze con i diritti e le libertà fondamentali dei lavoratori e non saranno costanti, prolungati e indiscriminati.
La generalizzazione di tali avvisi potrà riguardare l'intero insieme degli utenti (i.e. tramite flash news sulla intranet) o le aree logiche o fisiche in cui è stata rilevata l'anomalia. Negli avvisi, si evidenzierà l'utilizzo irregolare degli strumenti interaziendali e si inviteranno gli utenti del sistema informatico ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.
In caso siano rilevate ulteriori anomalie, le AASS potranno procedere con verifiche più specifiche e puntuali, anche su base individuale, qualora:

- accertino manomissioni alle configurazioni del sistema informatico, telematico interaziendale e/o accessi indebiti allo stesso;
- riscontrino diffusioni indebite di informazioni atte a pregiudicare la sicurezza del sistema informatico, telematico, o il suo buon funzionamento e/o ad estenderead altri soggetti accessi o privilegi non dovuti;
- abbiano concrete ragioni che portino a pensare che la sicurezza del sistema tecnologico interaziendale possa essere minacciata
- ravvisino un persistente utilizzo anomalo da parte degli utenti di una specifica struttura/area rilevabile attraverso il controllo anonimo

si riservano il diritto di:

- effettuare controlli specifici tesi ad accertare lo stato dei fatti relativamente all'uso delle attrezzature interaziendali;
- disabilitare le autorizzazioni all'accesso e all'uso delle attrezzature interaziendali;
- segnalare al delegato del trattamento dati situazioni e comportamenti anomali degli operatori.

In caso di problemi inerenti alla sicurezza della infrastruttura tecnologica, le AASS si riservano il diritto di adottare tutte le misure tecniche per garantire la gestione della contingenza. A mero titolo esemplificativo si riportano alcune misure:

- isolamento dalla rete delle stazioni che siano state infettate da virus e che ne pregiudichino il buon funzionamento;
- aggiornamento delle configurazioni software e/o
- sostituzioni hardware.

Tutte le azioni messe in atto dovranno essere valutate in una logica di costo/beneficio e saranno improntate ad un criterio di minimizzazione del disservizio.
Il SITI si riserva la possibilità di interrompere i servizi informatici per le manutenzioni ordinarie e straordinarie e per la gestione dei guasti, impegnandosi, tuttavia, nel limite del possibile, ad avvertire preventivamente gli utenti di dette interruzioni

7.3. Ulteriori accessi

Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware eccetera) o per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico eccetera), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà delle AASS, tramite il personale del SITI o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici gestiti dal SITI.

7.4. Sanzioni

È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente regolamento. Il mancato rispetto o la violazione delle regole sopra riportate da parte del personale a qualunque titolo autorizzato è perseguibile secondo la normativa vigente (disciplinare, amministrativa, civile e penale).
Si rammenta che il potere disciplinare non può comunque essere esercitato nei confronti dei collaboratori coordinati e continuativi, dei collaboratori a progetto e dei tirocinanti, mentre nei confronti dei lavoratori somministrati (ex interinali) va esercitato per il tramite dell'agenzia di somministrazione.
Con riferimento ai collaboratori, qualora questi per l'espletamento del loro incarico si servano degli strumenti considerati dal Regolamento, deve essere contrattualmente previsto l'obbligo di rispettare il Regolamento in questione.

7.5. Aggiornamento e revisione

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Regolamento. Le proposte verranno esaminate dal SITI e dal Gruppo Aziendale Privacy.

L'Informativa ai sensi dell'art. 13 del Regolamento (UE) 2016/679 riguardante il trattamento dei dati necessario ai fini del presente Regolamento, potrà essere visionata accedendo alla sezione privacy delle rispettive intranet aziendali.

GLOSSARIO

"**Trattamento":** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione
"**Dati personali ":** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
"**GDPR" o "Regolamento":** si intende il Regolamento UE 2016/679 sulla protezione delle persone fisiche relativamente al trattamento dei dati personali e della loro libera circolazione (General Data Protection Regulation) che sarà direttamente applicabile dal 25 maggio 2018.
"**Normativa Applicabile":** si intende l'insieme delle norme rilevanti in materia protezione dei dati personali , incluso il Regolamento Privacy UE 2016/679 (GDPR) ed ogni provvedimento del Garante per la protezione dei dati personali e del WP Art. 29.
"**Titolare del Trattamento":** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

“Delegato al trattamento”: persona fisica espressamente designata, interna all’organizzazione, che sotto l’autorità del titolare svolge specifici compiti e funzioni connessi al trattamento dei dati (generalmente, il Direttore della Struttura Complessa di afferenza, il Responsabile della Struttura Semplice Dipartimentale, altri soggetti designati in virtù di particolari compiti e funzioni attribuiti.
“Autorizzato”: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile del trattamento**.**
“Interessati”: le persone fisiche identificata o identificabile a cui si riferiscono i dati personali oggetto del trattamento.
.“**Responsabile del trattamento”**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
“**Pseudonimizzazione”**: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.
“**Garante per la protezione dei dati personali”:** è l’autorità di controllo responsabile per la protezione dei dati personali in Italia.