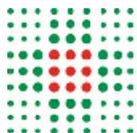


CODICE DI COMPORAMENTO: ASPETTI ICT

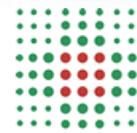
Marco Brambilla

*Direttore
Servizio Interaziendale Tecnologie dell'Informazione*

Illustrazione degli elementi di
contatto tra codice e
regolamento



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



**SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA**
Azienda Unità Sanitaria Locale di Parma

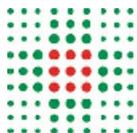
Sommario

- Il codice di comportamento
- Il Piano Interaziendale ICT
- Il regolamento ICT interaziendale

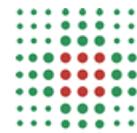


“ „Oggi siamo intrappolati in un mondo creato da tecnologi per altri tecnologi. Ci è stato persino detto che "essere digitali" costituisce una virtù. Non è vero: gli individui sono analogici, non digitali; biologici non meccanici.“ — ”

Donald Norman psicologo e ingegnere 1935
dalla prefazione della prima edizione di Il
computer invisibile



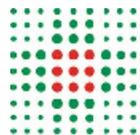
SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Ospedaliero - Universitaria di Parma



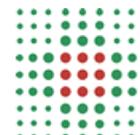
SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

Codice di comportamento

Il codice nella sua interezza



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



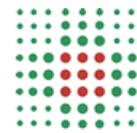
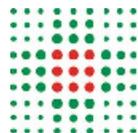
SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

Elementi di contatto

Il codice nella sua articolazione ha
numerosi punti a rilevanza ICT.

INDICE

Titolo I:	Disposizioni di carattere generale
Art. 1	Natura e finalità del Codice
Art. 2	Ambito di applicazione e definizioni
Titolo II:	Principi etici e valori di riferimento
Art. 3	Principi generali
Titolo III:	Norme di comportamento
Art. 4	Conflitto di interessi e obbligo di astensione
Art. 5	Regali, compensi e altre utilità
Art. 6	Partecipazione ad associazioni e organizzazioni
Art. 7	Prevenzione della corruzione
Art. 8	Trasparenza e tracciabilità
Art. 9	Comportamento nei rapporti privati
Art. 10	Comportamento in servizio e nei confronti del pubblico
Art. 11	Comportamento nell'utilizzo delle tecnologie informatiche, dei mezzi di informazione e dei social media
Art. 12	Disposizioni particolari per i dirigenti
Art. 13	Contratti e atti negoziali
Art. 14	Gestione delle liste di attesa e attività libero professionale
Art. 15	Ricerca e sperimentazioni
Art. 16	Sponsorizzazioni e attività formativa
Art. 17	Rapporti con società farmaceutiche e/o ditte produttrici di dispositivi medici
Art. 18	Attività conseguenti al decesso
Titolo IV:	Sistema sanzionatorio e di vigilanza
Art. 19	Vigilanza sull'applicazione del Codice
Art. 20	Responsabilità conseguenti alla violazione dei doveri del Codice e Disposizioni Sanzionatorie per i destinatari soggetti al potere disciplinare delle Aziende
Art. 21	Responsabilità conseguenti alla violazione dei doveri del Codice e Disposizioni Sanzionatorie per gli altri destinatari
Art. 22	Effetti del rispetto del Codice sul sistema di valutazione
Titolo V:	Disposizioni finali
Art. 23	Disposizioni finali
Allegato	Normativa di riferimento



Schema regionale

Il primo punto di contatto è lo schema di riferimento del codice di comportamento approvato da RER.

La RER coordina infatti il piano Digitale da cui discende il Piano ICT Interaziendale

INDICE



Titolo I:	Disposizioni di carattere generale
Art. 1	Natura e finalità del Codice
Art. 2	Ambito di applicazione e definizioni
Titolo II:	Principi etici e valori di riferimento
Art. 3	Principi generali
Titolo III:	Norme di comportamento
Art. 4	Conflitto di interessi e obbligo di astensione
Art. 5	Regali, compensi e altre utilità
Art. 6	Partecipazione ad associazioni e organizzazioni
Art. 7	Prevenzione della corruzione
Art. 8	Trasparenza e tracciabilità
Art. 9	Comportamento nei rapporti privati
Art. 10	Comportamento in servizio e nei confronti del pubblico
Art. 11	Comportamento nell'utilizzo delle tecnologie informatiche, dei mezzi di informazione e dei social media
Art. 12	Disposizioni particolari per i dirigenti
Art. 13	Contratti e atti negoziali
Art. 14	Gestione delle liste di attesa e attività libero professionale
Art. 15	Ricerca e sperimentazioni
Art. 16	Sponsorizzazioni e attività formativa
Art. 17	Rapporti con società farmaceutiche e/o ditte produttrici di dispositivi medici
Art. 18	Attività conseguenti al decesso
Titolo IV:	Sistema sanzionatorio e di vigilanza
Art. 19	Vigilanza sull'applicazione del Codice
Art. 20	Responsabilità conseguenti alla violazione dei doveri del Codice e Disposizioni Sanzionatorie per i destinatari soggetti al potere disciplinare delle Aziende
Art. 21	Responsabilità conseguenti alla violazione dei doveri del Codice e Disposizioni Sanzionatorie per gli altri destinatari
Art. 22	Effetti del rispetto del Codice sul sistema di valutazione
Titolo V:	Disposizioni finali
Art. 23	Disposizioni finali
Allegato	Normativa di riferimento

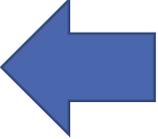
Ambito di applicazione

Ulteriore elemento di contatto è l'ambito di applicazione. Infatti

Il Codice si applica, salvo quanto disposto nei singoli articoli, a tutto il personale che a qualsiasi titolo presta attività lavorativa per le Aziende

Che risulta del tutto sovrapponibile all'ambito di applicazione del regolamento dei sistemi informatici

INDICE

Titolo I:	Disposizioni di carattere generale	
Art. 1	Natura e finalità del Codice	
Art. 2	Ambito di applicazione e definizioni	
Titolo II:	Principi etici e valori di riferimento	
Art. 3	Principi generali	
Titolo III:	Norme di comportamento	
Art. 4	Conflitto di interessi e obbligo di astensione	
Art. 5	Regali, compensi e altre utilità	
Art. 6	Partecipazione ad associazioni e organizzazioni	
Art. 7	Prevenzione della corruzione	
Art. 8	Trasparenza e tracciabilità	
Art. 9	Comportamento nei rapporti privati	
Art. 10	Comportamento in servizio e nei confronti del pubblico	
Art. 11	Comportamento nell'utilizzo delle tecnologie informatiche, dei mezzi di informazione e dei social media	
Art. 12	Disposizioni particolari per i dirigenti	
Art. 13	Contratti e atti negoziali	
Art. 14	Gestione delle liste di attesa e attività libero professionale	
Art. 15	Ricerca e sperimentazioni	
Art. 16	Sponsorizzazioni e attività formativa	
Art. 17	Rapporti con società farmaceutiche e/o ditte produttrici di dispositivi medici	
Art. 18	Attività conseguenti al decesso	
Titolo IV:	Sistema sanzionatorio e di vigilanza	
Art. 19	Vigilanza sull'applicazione del Codice	
Art. 20	Responsabilità conseguenti alla violazione dei doveri del Codice e Disposizioni Sanzionatorie per i destinatari soggetti al potere disciplinare delle Aziende	
Art. 21	Responsabilità conseguenti alla violazione dei doveri del Codice e Disposizioni Sanzionatorie per gli altri destinatari	
Art. 22	Effetti del rispetto del Codice sul sistema di valutazione	
Titolo V:	Disposizioni finali	
Art. 23	Disposizioni finali	
Allegato	Normativa di riferimento	

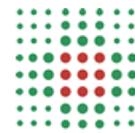
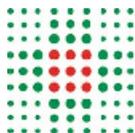
Ambito di applicazione

Ulteriore elemento di contatto è l'ambito di applicazione. Infatti

Il Codice si applica, salvo quanto disposto nei singoli articoli, a tutto il personale che a qualsiasi titolo presta attività lavorativa per le Aziende

Che risulta del tutto sovrapponibile all'ambito di applicazione del regolamento dei sistemi informatici

1. Il Codice si applica, salvo quanto disposto nei singoli articoli, a tutto il personale che a qualsiasi titolo presta attività lavorativa per le Aziende e nello specifico a:
 - a) dipendenti con rapporto di lavoro a tempo indeterminato e determinato
 - b) dipendenti di altre pubbliche amministrazioni in comando, distacco o fuori ruolo
 - c) collaboratori e consulenti dell'Azienda con qualsiasi tipologia di contratto e incarico, conferito a qualsiasi titolo
 - d) medici e altro personale universitario integrati per l'assistenza; personale universitario non in convenzione assistenziale ai sensi del decreto legislativo n. 517/1999 che svolge attività di ricerca
 - e) medici di medicina generale, medici di continuità assistenziale, medici dei servizi territoriali, medici dell'emergenza sanitaria territoriale, pediatri di libera scelta e specialisti ambulatoriali interni (medici, veterinari, biologi, chimici, psicologi) per quanto compatibile con le convenzioni vigenti
 - f) medici in formazione specialistica, ricercatori a tempo determinato e/o con contratti flessibili, dottorandi, assegnisti di ricerca autorizzati allo svolgimento delle attività assistenziali e di ricerca e tirocinanti
 - g) direttore generale, amministrativo, sanitario, scientifico, assistenziale e socio-sanitario ove presenti
 - h) personale a qualsiasi titolo di imprese fornitrici di beni, servizi o lavori, in conformità con quanto previsto dai Patti di integrità dagli stessi sottoscritti
 - i) volontari componenti di associazioni di volontariato, in conformità con quanto previsto dagli accordi dalle stesse sottoscritte.
2. A tal fine, nei provvedimenti di incarico o nei contratti di collaborazione, consulenza o servizio, sono inserite apposite clausole di risoluzione del rapporto di lavoro, di decadenza o altre disposizioni in caso di violazione degli obblighi derivanti dal presente Codice e/o dal Regolamento, secondo quanto previsto dagli artt. 20 e 21.
3. Le Società controllate o partecipate dalle Aziende, e i loro dipendenti, nell'applicazione della normativa in materia sono destinatarie del presente Codice in termini di principi ed indirizzi.



Uso delle risorse

Nei principi generali, al punto m, esplicita
l'uso delle risorse pubbliche

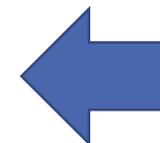
m) Uso delle risorse pubbliche

*1. Le Aziende assicurano che gli arredi, il
materiale, le attrezzature, gli strumenti
tecnologici e informatici e, più in generale,
qualsiasi risorsa, sia utilizzata con scrupolo,
cura e diligenza.*

Che, oltre ai richiami al regolamento IT,
risulta congruente con i regolamenti relativi
alla gestione dei beni / figure di
consegnatario

INDICE

Titolo I:	Disposizioni di carattere generale
Art. 1	Natura e finalità del Codice
Art. 2	Ambito di applicazione e definizioni
Titolo II:	Principi etici e valori di riferimento
Art. 3	Principi generali
Titolo III:	Norme di comportamento
Art. 4	Conflitto di interessi e obbligo di astensione
Art. 5	Regali, compensi e altre utilità
Art. 6	Partecipazione ad associazioni e organizzazioni
Art. 7	Prevenzione della corruzione
Art. 8	Trasparenza e tracciabilità
Art. 9	Comportamento nei rapporti privati
Art. 10	Comportamento in servizio e nei confronti del pubblico
Art. 11	Comportamento nell'utilizzo delle tecnologie informatiche, dei mezzi di informazione e dei social media
Art. 12	Disposizioni particolari per i dirigenti
Art. 13	Contratti e atti negoziali
Art. 14	Gestione delle liste di attesa e attività libero professionale
Art. 15	Ricerca e sperimentazioni
Art. 16	Sponsorizzazioni e attività formativa
Art. 17	Rapporti con società farmaceutiche e/o ditte produttrici di dispositivi medici
Art. 18	Attività conseguenti al decesso
Titolo IV:	Sistema sanzionatorio e di vigilanza
Art. 19	Vigilanza sull'applicazione del Codice
Art. 20	Responsabilità conseguenti alla violazione dei doveri del Codice e Disposizioni Sanzionatorie per i destinatari soggetti al potere disciplinare delle Aziende
Art. 21	Responsabilità conseguenti alla violazione dei doveri del Codice e Disposizioni Sanzionatorie per gli altri destinatari
Art. 22	Effetti del rispetto del Codice sul sistema di valutazione
Titolo V:	Disposizioni finali
Art. 23	Disposizioni finali
Allegato	Normativa di riferimento



Tracciabilità

L'articolo 8, in particolare al comma 2, sottolinea l'importanza della tracciabilità dei processi decisionali.

INDICE

Titolo I:	Disposizioni di carattere generale
Art. 1	Natura e finalità del Codice
Art. 2	Ambito di applicazione e definizioni
Titolo II:	Principi etici e valori di riferimento
Art. 3	Principi generali
Titolo III:	Norme di comportamento
Art. 4	Conflitto di interessi e obbligo di astensione
Art. 5	Regali, compensi e altre utilità
Art. 6	Partecipazione ad associazioni e organizzazioni
Art. 7	Prevenzione della corruzione
Art. 8	Trasparenza e tracciabilità
Art. 9	Comportamento nei rapporti privati
Art. 10	Comportamento in servizio e nei confronti del pubblico
Art. 11	Comportamento nell'utilizzo delle tecnologie informatiche, dei mezzi di informazione e dei social media
Art. 12	Disposizioni particolari per i dirigenti
Art. 13	Contratti e atti negoziali
Art. 14	Gestione delle liste di attesa e attività libero professionale
Art. 15	Ricerca e sperimentazioni
Art. 16	Sponsorizzazioni e attività formativa
Art. 17	Rapporti con società farmaceutiche e/o ditte produttrici di dispositivi medici
Art. 18	Attività conseguenti al decesso
Titolo IV:	Sistema sanzionatorio e di vigilanza
Art. 19	Vigilanza sull'applicazione del Codice
Art. 20	Responsabilità conseguenti alla violazione dei doveri del Codice e Disposizioni Sanzionatorie per i destinatari soggetti al potere disciplinare delle Aziende
Art. 21	Responsabilità conseguenti alla violazione dei doveri del Codice e Disposizioni Sanzionatorie per gli altri destinatari
Art. 22	Effetti del rispetto del Codice sul sistema di valutazione
Titolo V:	Disposizioni finali
Art. 23	Disposizioni finali
Allegato	Normativa di riferimento

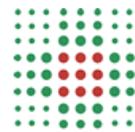
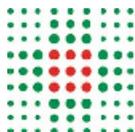
Tracciabilità

Il parallelismo con il fronte ICT prosegue con il rispetto delle diverse istruzioni operative che regolano i sistemi ICT.

Particolare importanza, per il rispetto di questo articolo, è ad esempio rivestita dal manuale di gestione dei flussi documentali.

Art. 8 Trasparenza e tracciabilità

1. I destinatari del Codice, secondo quanto previsto nella Sottosezione Rischi Corruttivi e Trasparenza del PIAO interaziendale, assicurano l'adempimento degli obblighi di trasparenza previsti in capo alle pubbliche amministrazioni in conformità alle disposizioni normative vigenti, anche prestando la massima collaborazione nell'elaborazione, reperimento e trasmissione dei dati sottoposti all'obbligo di pubblicazione sui siti istituzionali "Amministrazione Trasparente".
2. La tracciabilità dei processi decisionali adottati deve essere, in tutti i casi, garantita attraverso un adeguato supporto documentale ed informatico, che consenta in ogni momento la replicabilità del processo decisionale, assicurando la completezza e l'integrità della documentazione amministrativa e/o sanitaria, con un linguaggio chiaro e comprensibile. Deve essere garantita la conservazione dei documenti acquisiti e prodotti ai fini della rintracciabilità del relativo fascicolo e della documentazione in generale.
3. La tenuta e la conservazione della documentazione amministrativa e/o sanitaria deve avvenire nel rispetto della normativa privacy.
4. I destinatari concorrono a garantire la piena attuazione del diritto di accesso documentale, civico e generalizzato, in ottemperanza alle disposizioni legislative e regolamentari vigenti.



Utilizzo tecnologie

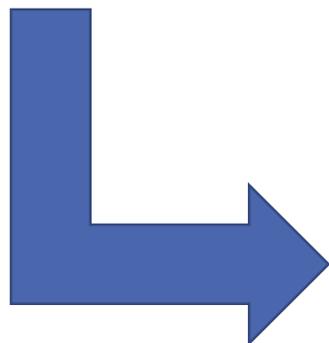
L'articolo 11 sintetizza, in particolare nei commi 1,2,3 e 4, i principi generali del regolamento interaziendale sull'utilizzo dei sistemi informatici

INDICE

Titolo I:	Disposizioni di carattere generale
Art. 1	Natura e finalità del Codice
Art. 2	Ambito di applicazione e definizioni
Titolo II:	Principi etici e valori di riferimento
Art. 3	Principi generali
Titolo III:	Norme di comportamento
Art. 4	Conflitto di interessi e obbligo di astensione
Art. 5	Regali, compensi e altre utilità
Art. 6	Partecipazione ad associazioni e organizzazioni
Art. 7	Prevenzione della corruzione
Art. 8	Trasparenza e tracciabilità
Art. 9	Comportamento nei rapporti privati
Art. 10	Comportamento in servizio e nei confronti del pubblico
Art. 11	Comportamento nell'utilizzo delle tecnologie informatiche, dell'informazione e dei social media
Art. 12	Disposizioni particolari per i dirigenti
Art. 13	Contratti e atti negoziali
Art. 14	Gestione delle liste di attesa e attività libero professionale
Art. 15	Ricerca e sperimentazioni
Art. 16	Sponsorizzazioni e attività formativa
Art. 17	Rapporti con società farmaceutiche e/o ditte produttrici di dispositivi medici
Art. 18	Attività conseguenti al decesso
Titolo IV:	Sistema sanzionatorio e di vigilanza
Art. 19	Vigilanza sull'applicazione del Codice
Art. 20	Responsabilità conseguenti alla violazione dei doveri del Codice e Disposizioni Sanzionatorie per i destinatari soggetti al potere disciplinare delle Aziende
Art. 21	Responsabilità conseguenti alla violazione dei doveri del Codice e Disposizioni Sanzionatorie per gli altri destinatari
Art. 22	Effetti del rispetto del Codice sul sistema di valutazione
Titolo V:	Disposizioni finali
Art. 23	Disposizioni finali
Allegato	Normativa di riferimento

Utilizzo tecnologie

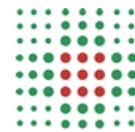
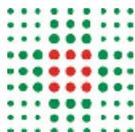
L'articolo 11 sintetizza, in particolare nei commi 1,2,3 e 4, i principi generali del regolamento interaziendale sull'utilizzo dei sistemi informatici



1. Nell'utilizzo delle tecnologie informatiche messe a disposizione dalle Aziende per lo svolgimento dell'attività di servizio, anche nella modalità a distanza, i destinatari del Codice rispettano i regolamenti aziendali in materia.

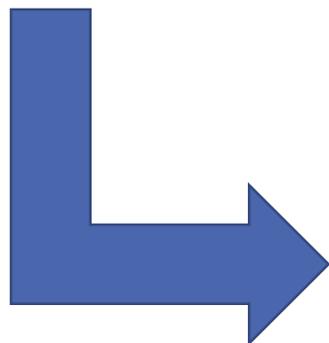
In particolare, i destinatari del Codice:

- a. perseguono esclusivamente le finalità aziendali cui le tecnologie sono destinate, secondo le autorizzazioni ricevute ed attenendosi ai principi diligenza, correttezza, necessità, indispensabilità e non eccedenza
- b. adottano ogni misura per proteggere le tecnologie ed i sistemi informatici da eventuali danneggiamenti, furti od altri eventi che possano pregiudicare le attività aziendali
- c. adottano ogni utile misura di sicurezza atta ad evitare che le credenziali di autenticazione ai sistemi informatici aziendali vengano a conoscenza di altri soggetti. L'eventuale uso improprio di apparecchiature, strumenti o servizi sarà imputato al titolare delle credenziali tramite le quali l'accesso è avvenuto
- d. accedono alla rete Internet esclusivamente mediante il Provider scelto ufficialmente dalle Aziende, nell'ambito dello svolgimento delle attività assegnate.

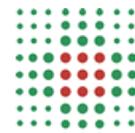
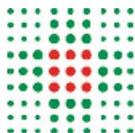


Utilizzo tecnologie

L'articolo 11 sintetizza, in particolare nei commi 1,2,3 e 4, i principi generali del regolamento interaziendale sull'utilizzo dei sistemi informatici

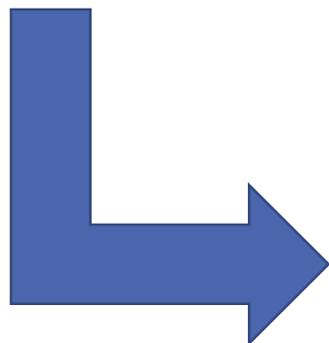


2. È consentito l'utilizzo degli strumenti informatici forniti dalle Aziende per poter assolvere alle incombenze personali senza doversi allontanare dalla sede di servizio, purché l'attività sia contenuta in tempi ristretti e senza alcun pregiudizio per i compiti istituzionali. In ogni caso, è fatto divieto di utilizzare strumenti informatici forniti dall'amministrazione per fini diversi da quelli connessi all'attività lavorativa o ad essa riconducibili nel caso in cui l'utilizzo possa compromettere la sicurezza o la reputazione dell'Azienda.

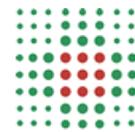
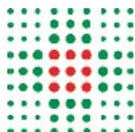


Utilizzo tecnologie

L'articolo 11 sintetizza, in particolare nei commi 1,2,3 e 4, i principi generali del regolamento interaziendale sull'utilizzo dei sistemi informatici

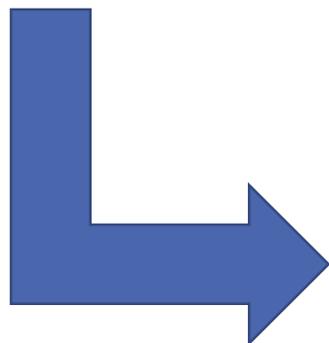


3. Le Aziende svolgono gli accertamenti necessari e adottano ogni misura atta a garantire la sicurezza e la protezione dei sistemi informatici, delle informazioni e dei dati, secondo le modalità previste dai regolamenti aziendali in materia e in relazione alla tutela della riservatezza dei dati personali e particolari.



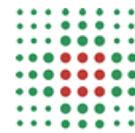
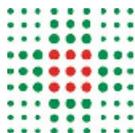
Utilizzo tecnologie

L'articolo 11 sintetizza, in particolare nei commi 1,2,3 e 4, i principi generali del regolamento interaziendale sull'utilizzo dei sistemi informatici



4. I Destinatari del codice, per le comunicazioni aziendali:

- a. utilizzano esclusivamente l'indirizzo di posta elettronica aziendale e sono responsabili del contenuto dei messaggi inviati



Utilizzo tecnologie



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

A tutti i Direttori/Responsabili di S.C., SSD,
SS di U.O., e programmi equivalenti

Direzione Sanitaria

E p.c.

Il Direttore Sanitario

Al Direttore Generale
Al Direttore Amministrativo
Al Direttore Servizio Assistenziale
Al Responsabile SS Medicina Legale
Al Direttore Servizio Informativo Aziendale

AZOSPR

USCITA - 20/12/2017 - 0047262 - 1.1.6



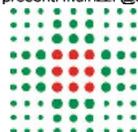
Loro Sedi

Oggetto: comunicazione mediante mail e liste di distribuzione.

Con la presente si coglie l'occasione per ricordare alle SS.LL., in qualità di Responsabili al trattamento dati personali individuati ai sensi del Regolamento Aziendale per la tutela della riservatezza nel trattamento dei dati personali e sensibili (approvato con deliberazione del Direttore Generale n. 22 del 26/01/2010) e a cui è ascritta la responsabilità della corretta gestione dei dati, che le SS.LL. sono tenute a compiere tutto quanto è necessario per il rispetto delle vigenti disposizioni in tema di riservatezza.

In particolare le SS.LL. hanno il dovere di osservare e fare osservare le disposizioni aziendali in tema di riservatezza (nomina incaricati, conservazione dei dati, ecc.) nonché in tema di utilizzo degli strumenti informatici e, nella fattispecie, delle caselle di posta elettronica e delle liste di distribuzione.

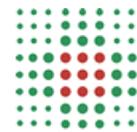
Richiamando il "Regolamento per l'utilizzo dei sistemi informatici dell'Azienda Ospedaliero - Universitaria di Parma" (approvato con deliberazione del Direttore Generale n. 108 del 15/03/2016) la casella di posta elettronica aziendale, che costituisce uno strumento di lavoro, impegna ogni Professionista a farne congruo utilizzo per la corrispondenza, e a provvedere alla costante manutenzione della stessa; essa è assegnata ai dipendenti e ne è vietato l'utilizzo personale e non istituzionale. L'Azienda riconosce inoltre, in virtù della propria natura ospedaliero-universitaria, gli indirizzi di posta elettronica dell'Università degli Studi di Parma come indirizzi mail istituzionali dei Professionisti convenzionati. Nella rubrica aziendale sono pertanto presenti indirizzi @ao.pr.it e indirizzi @unipr.it.



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

4. I Destinatari del codice, per le comunicazioni aziendali:

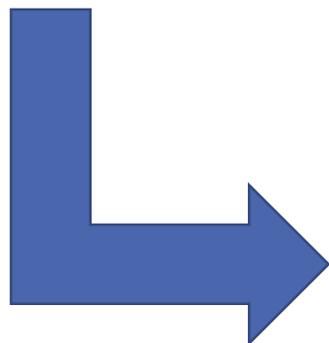
- utilizzano esclusivamente l'indirizzo di posta elettronica aziendale e sono responsabili del contenuto dei messaggi inviati



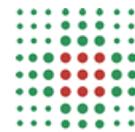
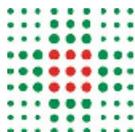
SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

Utilizzo tecnologie

L'articolo 11 sintetizza, in particolare nei commi 1,2,3 e 4, i principi generali del regolamento interaziendale sull'utilizzo dei sistemi informatici



- b. utilizzano gli account istituzionali per i soli fini connessi all'attività lavorativa o ad essa riconducibili e non possono compromettere in alcun modo la sicurezza o la reputazione dell'Azienda; di norma evitano l'utilizzo di caselle di posta elettronica personali per attività o comunicazioni afferenti al servizio salvi i casi di forza maggiore dovuti a circostanze in cui il dipendente, per qualsiasi ragione, non possa accedere all'account istituzionale



Utilizzo tecnologie

Da: presidente@pec.governo.it

A: info@pizzeriadontonino.it

Oggetto: prenotazione

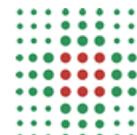
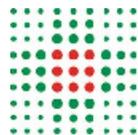
Buonasera,

si richiede di riservare un tavolo per 4 stasera alle ore 21 a nome Matterella.

Saluti

Sergio

- b. utilizzano gli account istituzionali per i soli fini connessi all'attività lavorativa o ad essa riconducibili e non possono compromettere in alcun modo la sicurezza o la reputazione dell'Azienda; di norma evitano l'utilizzo di caselle di posta elettronica personali per attività o comunicazioni afferenti al servizio salvi i casi di forza maggiore dovuti a circostanze in cui il dipendente, per qualsiasi ragione, non possa accedere all'account istituzionale



Utilizzo tecnologie



COMUNICATO STAMPA DEL 29 NOVEMBRE 2023

Attacco hacker ai sistemi delle tre Aziende sanitarie modenesi

Informazioni utili per i cittadini

[Aggiornamento delle ore 17:00 del 29/11/23: l'elenco dei servizi garantiti per domani e indicazioni ai cittadini](#)

Fin dalle prime ore di questa mattina e nel corso della giornata si sono riunite le task force delle Aziende sanitarie modenesi per garantire la gestione dell'attacco hacker subito nel corso della notte; un gruppo di coordinamento interaziendale è tuttora impegnato per la risoluzione dei problemi che si sono creati. Le Aziende stanno lavorando assiduamente per il progressivo ripristino dei sistemi che sono stati isolati per mantenere la sicurezza delle informazioni ed evitare la propagazione dell'attacco.

Sulla home page del portale AUSL sarà a disposizione da ora il costante aggiornamento sulla situazione dei servizi. Si invitano i cittadini a consultare periodicamente la pagina www.ausl.mo.it e le pagine di AOU (www.aou.mo.it) e Ospedale di Sassuolo Spa (www.ospedalesassuolo.it).

- b. utilizzano gli account istituzionali per i soli fini connessi all'attività lavorativa o ad essa riconducibili e non possono compromettere in alcun modo la sicurezza o la reputazione dell'Azienda; di norma evitano l'utilizzo di caselle di posta elettronica personali per attività o comunicazioni afferenti al servizio salvi i casi di forza maggiore dovuti a circostanze in cui il dipendente, per qualsiasi ragione, non possa accedere all'account istituzionale

Utilizzo tecnologie

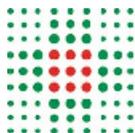
L'articolo 11 sintetizza, in particolare nei commi 1,2,3 e 4, i principi generali del regolamento interaziendale sull'utilizzo dei sistemi informatici

Ing. Ph.D. Marco Brambilla
Direttore
Servizio Interaziendale Tecnologie dell'Informazione
Azienda (Ospedaliero - Universitaria | USL) di Parma

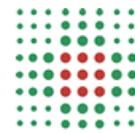
tel: +39 0521 704510
mail: mbrambilla@ao.pr.it

Disclaimer : The information contained in this e-mail is intended only for the individual addressed. If you have received this e-mail by mistake, please notify us immediately by return reply. Be sure to delete this message and all its attachments from your system. Please note that any unauthorized review, copying, disclosure or any other use of this information is strictly prohibited. E-mail transmission cannot be guaranteed to be secure or error-free as information could be intercepted, corrupted, lost, destroyed, received late or incomplete, or could contain viruses. The sender therefore does not accept any liability for any error or omission in the content of this message, either of which are caused as a result of e-mail transmission.

c. si uniformano alle modalità di firma dei messaggi di posta elettronica di servizio individuate dalle Aziende. Ciascun messaggio in uscita deve consentire l'identificazione del mittente e deve indicare un recapito istituzionale al quale il medesimo è reperibile.



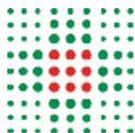
SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Ospedaliero - Universitaria di Parma



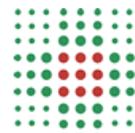
SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

Il Piano ICT Interaziendale

I punti salienti del triennio 2022-2024



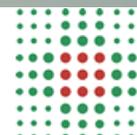
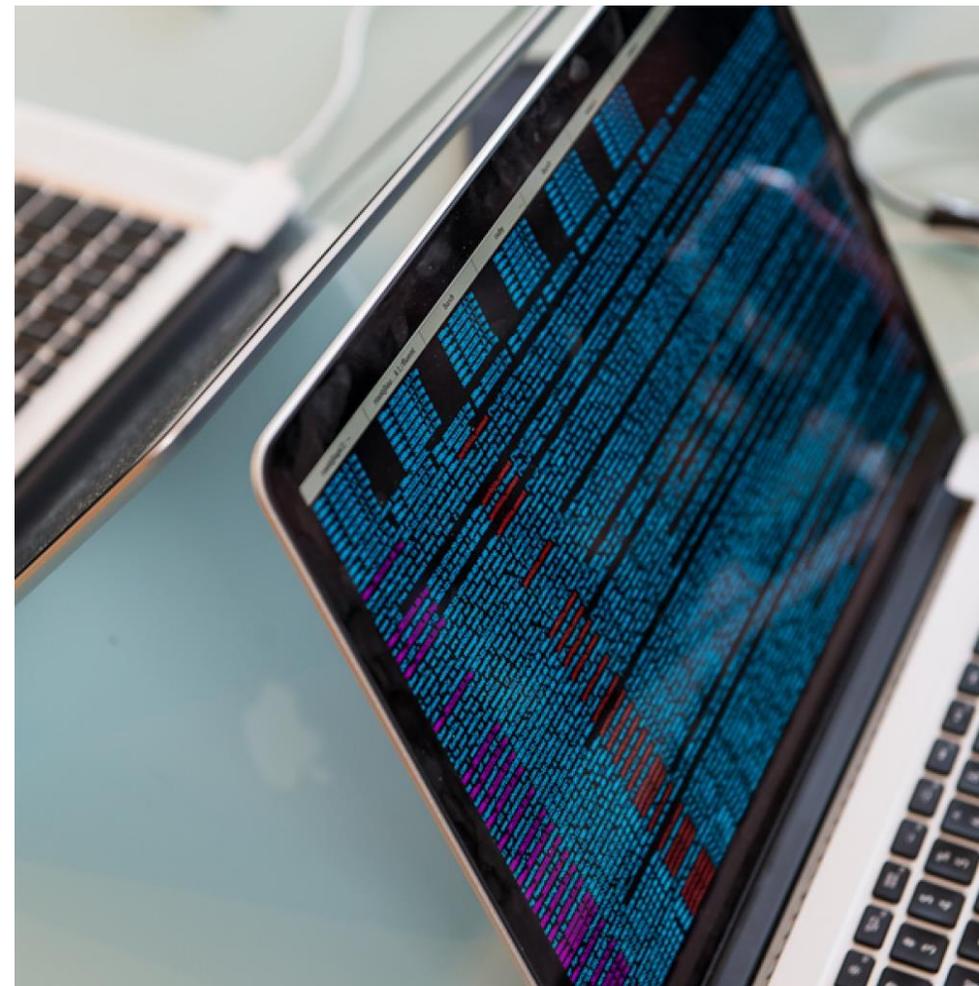
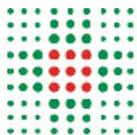
SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Ospedaliero - Universitaria di Parma



SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

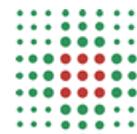
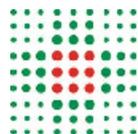
La relazione al Piano ICT

- A termine di ogni anno deve essere redatta una relazione al Piano che dovrà poi essere a disposizione di AGID e del Difensore Civico Digitale
- RTD chiederà ad ogni articolazione individuata nel piano una relazione di riscontro sul raggiungimento degli obiettivi specificatamente assegnati o comunque un'evidenza del mancato raggiungimento con le specifiche motivazioni (es. proroga normativa).
- Sulla base degli esiti del piano dell'anno precedente, dell'aggiornamento del piano nazionale e regionale, l'anno successivo verrà aggiornato il piano triennale.



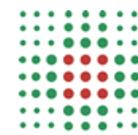
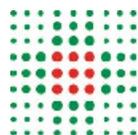
Principali elementi

- Ufficio Comunicazione: utilizza Web Analytics Italia per migliorare il processo evolutivo dei propri servizi online.
- SITI acquisisce servizi cloud solo se qualificati da AGID, consultando il Catalogo dei servizi cloud qualificati da AGID per la PA.
- SITI dichiara, all'interno del catalogo di Developers Italia, quali software di titolarità di un'altra PA hanno preso in riuso.
- SAB e SITI: utilizzano procedure di procurement aderenti alle linee guida di AGID sull'acquisizione del software e al CAD (artt. 68 e 69).
- SITI: in accordo con il Piano ICT Regionale prosegue la migrazione al cloud.
- SITI pubblica (entro marzo) gli obiettivi di accessibilità sul proprio sito -
- SITI raccoglie (entro aprile) il software di cui risulta titolare ed esegue il rilascio in open source in ottemperanza dell'obbligo previsto dall'art. 69 CAD e secondo le procedure indicate nelle Linee guida attuative su acquisizione e riuso del software.
- SITI pubblica, entro il 23 giugno, la dichiarazione di accessibilità per le eventuali APP mobili, tramite l'applicazione form.agid.gov.it



Principali elementi

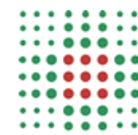
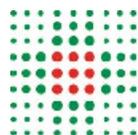
- SITI termina adeguamento dei sistemi di refertazione al fine di inviare documenti compliant con CDA2 per piattaforma FSE/INI;
- SIC termina adeguamento dei sistemi di refertazione al fine di inviare documenti compliant con CDA2 per piattaforma FSE/INI;
- Direzioni Sanitarie, in accordo a tutti i dipartimenti di erogazione di prestazioni (ambulatoriale, ALP, sanità pubblica...) rivede percorsi ed utilizzo del sistema CUP provinciale per la prenotazione di tutte le prestazioni ambulatoriali per esterni ivi comprese le prestazioni di chirurgia ambulatoriale e laboratorio anche attraverso la piattaforma FSE.
- Gruppo Privacy (in seduta interaziendale) fornisce istruzioni alle strutture che trattano dati genetici al fine della pubblicazione su FSE/INI;
- Gruppo Privacy (in seduta interaziendale) e SITI partecipano al processo di analisi e attivazione dell'invio al FSE del referto di Anatomia Patologica;
- SIC definisce un piano triennale interaziendale di interfacciamento delle tecnologie sanitarie che prevedono l'emissione di tracciati e/o informazioni cliniche rilevanti al fine della refertazione, con i sistemi informativi aziendali.
- SITI promuove l'accesso al FSE dei cittadini con la nuova modalità SIRD e al portale FSE Professionisti
- Direzioni Amministrative inseriscono obbligo e specifiche clausole negli accordi con il private accreditato dell'alimentazione del FSE, dell'utilizzo del sistema CUP per prenotazione, accettazione ed erogazione tramite il sistema della ricetta dematerializzata anche ai fini del riconoscimento economico delle prestazioni.



Principali elementi

Piattaforme CUP, SPID e PagoPA

- Gestione Amministrative delle Prestazioni Sanitarie ed Accessibilità, inseriscono le agende di ALP nel sistema CUP interaziendale connesse al sistema di gestione ALP.
- SITI e Servizio Interaziendale Accessibilità avviano piano di dismissione del sistema CUP Forms a favore del sistema Web.
- SITI prosegue il percorso di adesione a SPID e dismette le altre modalità di autenticazione relative ai servizi online (sistema informatico Emofilia)
- SITI entro giugno trasmette a RER i servizi online che eroga anche a minori attraverso SPID ai fini della rilevazione AGID
- Servizio Economico Finanziario e servizi amministrativi coinvolti proseguono nell'accettazione esclusiva dei pagamenti tramite PagoPA.

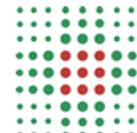
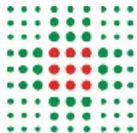


Regolamento Interaziendale

Dai due sistemi informatici ad un sistema informatico interaziendale

Origini...

- AO - 10 Ottobre 2012, delibera 257
 - Regolamento per l'utilizzo dei sistemi informatici di concerto con referente privacy
- AO - 12 Marzo 2016, delibera 108
 - Aggiornamento del regolamento di concerto con referente privacy
- 2018 => GDPR
- AUSL arriva referente privacy e arrivano prime circolari e indicazioni in attesa di un documento «padre»



Origini...

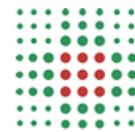
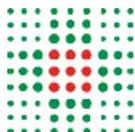
- Per ognuno dei punti oggetto del regolamento vi è stato, con i referenti privacy, alla luce delle indicazioni della DPO
 - un dibattito
 - un'analisi sulle modalità di recepimento delle indicazioni GDPR
 - il percorso di condivisione sindacale
 - un'adozione finale

Credenziali

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.



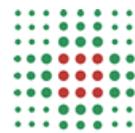
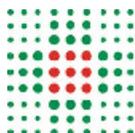
Credenziali

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.



Accesso ai sistemi informatici

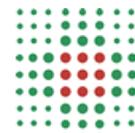
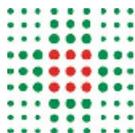
3.3. Richiesta, modifica e revoca delle abilitazioni ai sistemi informatici

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).



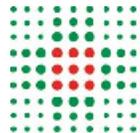
Posta elettronica

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 servizi.

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)

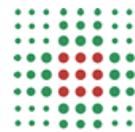
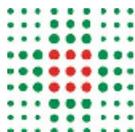


Cartella personale

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

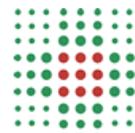
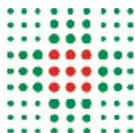


Cartella condivisa

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).



Misure di sicurezza

5.6. Misure di sicurezza e Piano ICT

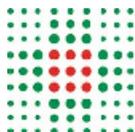
Il sistema informatico interaziendale è oggetto di continuo intervento per la salvaguardia della sicurezza dello stesso. In particolare sono perseguite le misure di sicurezza AGID tra cui, sono richiamati di seguito, alcuni dei principali elementi di riflesso sull'utente del sistema informatico interaziendale.

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 obiettivi 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.



Smartworking

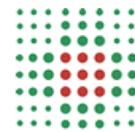
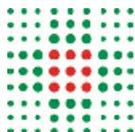
5.7. Tecnologie informatiche personali e accessi da remoto

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.

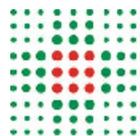
Per il personale afferente alle AASS (vedi paragrafo 4.1) l'accesso avviene tramite VPN via Https (c.d. Smartworking web).

Il collaboratore che si connette al precitato sistema garantisce che:

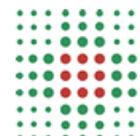
- la tecnologia informatica personale (es. PC o tablet) risponde in tutto e per tutto alle misure di sicurezza AGID al livello adeguate al trattamento in essere;
- effettuerà stampe locali al proprio PC solo di documenti privi di dati personali;
- non effettuerà esportazioni o salvataggi locali di dati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



Lavori in corso

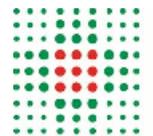


SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Ospedaliero - Universitaria di Parma



SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

QUESTIONS & ANSWERS



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



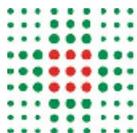
**SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA**
Azienda Unità Sanitaria Locale di Parma

CODICE DI COMPORAMENTO: ASPETTI ICT

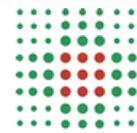
Marco Brambilla

*Direttore
Servizio Interaziendale Tecnologia dell'Informazione*

Illustrazione degli elementi di
contatto tra codice e
regolamento dei sistemi
informatici



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



**SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA**
Azienda Unità Sanitaria Locale di Parma