REGIONE AUTONOMA FRIULI VENEZIA GIULIA
ente per la gestione accentrata dei servizi condivisi
EGAS

Policy EGAS per l'utilizzo delle risorse informatiche

MATRICE DELLE REVISIONI					
REVISIONE	DATA	DESCRIZIONE / TIPO MODIFICA	REDATTA DA	VERIFICATA DA	APPROVATA DA
00	05/09/2017	Emissione	Servizio Informativo Carlo De Angelis Servizio Informativo Nicola Bortolotti	Direttore Amministrativo Tecla Del Do Direttore SC Economico Finanziaria Nives Di Marco Politiche e Gestione Risorse Umane Daniela Martini Affari Generali Alessandro Camarda, Sonia Borghese	Direttore Generale Massimo Romano
01	10/12/2018	Prima Revisione	Servizio Informativo Nicola Bortolotti	Direttore Amministrativo Tecla Del Do Direttore SC Economico Finanziaria Nives Di Marco Politiche e Gestione Risorse Umane Daniela Martini Affari Generali Alessandro Camarda, Sonia Borghese	Direttore Generale Massimo Romano
02					
03					
04					
05					

Approvato con decreto n. del

1 Indice

2 Premessa

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, l'accesso alla rete Internet dai Personal Computer, espone Egas e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e legge sulla privacy, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine dell'Azienda stessa. In questo senso viene fortemente sentita la necessità di porre in essere adeguati sistemi di controllo sull'utilizzo di tali strumenti da parte dei dipendenti e di sanzionare, conseguentemente, eventuali usi scorretti.
Premesso, quindi, che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, Egas ha adottato una policy interna diretta ad evitare che determinati comportamenti possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati. I controlli sull'uso degli strumenti informatici devono garantire tanto il diritto del datore di lavoro di proteggere la propria organizzazione - essendo le dotazioni oggetto della presente policy strumenti di lavoro la cui utilizzazione personale è preclusa - quanto il diritto del lavoratore a non vedere invasa la propria sfera personale ed il conseguente diritto alla riservatezza ed alla dignità, così come sanciti dallo Statuto dei Lavoratori e dal d.lgs. 196/03 e ss.mm.ii.
Questo regolamento viene incontro a tali esigenze disciplinando le condizioni per il corretto utilizzo degli strumenti informatici e/o telematici, anche alla luce degli obblighi previsti nel disciplinare tecnico in materia di Misure Minime di Sicurezza (richiamate con il carattere sottolineato), fornendo informazioni in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse.
L'inosservanza delle prescrizioni può comportare sanzioni di natura civile e penale per l'incaricato e per l'azienda, per cui si raccomanda di prestare la massima attenzione nella lettura delle disposizioni di seguito riportate.

3 Finalità

Considerato che l'Ente per la Gestione Accentrata dei Servizi Condivisi - nel seguito per brevità "EGAS" - nell'ottica di uno svolgimento proficuo e più agevole della propria attività, mette a disposizione dei propri dipendenti e collaboratori, apparecchiature informatiche e mezzi di comunicazione (Personal Computer, Notebook, Tablet, accesso alla rete aziendale, accesso alle procedure aziendali, casella di posta elettronica, accesso alla rete Internet, etc.), la presente policy ha l'obiettivo di:

- regolamentare l'utilizzo dei sistemi informatici, di Internet e della posta elettronica per garantire la sicurezza e prevenire il danneggiamento delle risorse informatiche Aziendali. Le prescrizioni sono impartite tenendo conto del diritto di protezione dei dati personali (nell'osservanza dei principi di necessità, correttezza, finalità determinate, esplicite e legittime) e osservando il principio di pertinenza e non eccedenza;
- adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e di dati, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità;
- tutelare il lavoratore;
- informare i dipendenti sul trattamento dei dati connesso all'attività di verifica e controllo.

Le disposizioni contenute potranno essere aggiornate alla luce dell'esperienza e dell'innovazione tecnologica.

4 Ambiti di applicazione

Il documento è redatto in conformità ai principi di cui all'art.4 della Legge n.300/1970, nonché in applicazione della Deliberazione Garante "Linee Guida per posta elettronica e internet" del 10 marzo 2007.
I rapporti tra l'Azienda e l'utenza si ispirano a principi di trasparenza e leale collaborazione.
Questa Policy si applica a:

- a tutto il personale dipendente ed al personale autorizzato che utilizza le risorse informatiche dell'Azienda a prescindere dal rapporto contrattuale con la stessa intrattenuto (dipendenti a tempo pieno o parziale, collaboratori, consulenti, medici in formazione, borsisti, tirocinanti, docenti, studenti, dottorandi, volontari di associazioni, dipendenti di aziende esterne legate da contratti di fornitura di servizi o altri individui a cui ne è concesso l'uso), senza distinzione di ruolo e/o livello;
- tutte le risorse informatiche e le tecnologie (personal computer, smartphone, cartelle condivise, sistemi di autenticazione, ecc.) di proprietà dell'Azienda e/o messe a disposizione dall'Egas o nell'ambito del Sistema Informativo Socio-Sanitario Regionale (in seguito SISSR);
- tutti i servizi e le operazioni di accesso a informazioni registrate ed archiviate elettronicamente tramite risorse informatiche aziendali;
- tutte le attività o forme di comunicazione operate attraverso l'utilizzo della rete e della posta elettronica, mediante strumentazione aziendale o di terze parti autorizzate all'uso dell'infrastruttura aziendale.

5 Direttive

5.1 Utilizzi consentiti

Le risorse informatiche aziendali sono strumenti di lavoro e come tali possono essere utilizzate solo per scopi strettamente professionali e lavorativi compresi quelli di ricerca e di didattica.

Il personale interessato dalle disposizioni della presente Policy, è tenuto a contattare il Servizio Informativo prima di intraprendere qualsiasi attività tecnica non esplicitamente contenuta nella presente Policy, al fine di garantire che tali attività non siano in contrasto con gli standard di sicurezza informatica stabiliti dall'Azienda.

- È vietata la connessione alla rete aziendale di qualsiasi dispositivo non preventivamente autorizzato dal Servizio Informativo

Il collegamento dei dispositivi alla rete aziendale deve essere autorizzato dal Servizio Informativo secondo le modalità previste dalle procedure in essere "MODALITÀ OPERATIVE PER IL COLLEGAMENTO DI NUOVI DISPOSITIVI ALLA RETE EGAS"; in assenza di autorizzazione è fatto divieto tassativo di connettere alla rete qualsiasi tipologia di apparato.
La procedura per il collegamento in rete di un nuovo dispositivo prevede il cambio delle credenziali dell'amministratore predefinito del dispositivo.

I dispositivi informatici sono affidati al personale dietro esplicita e preventiva richiesta da parte del dirigente delegato della struttura di appartenenza.
Il Servizio Informativo valuta periodicamente lo stato di obsolescenza del materiale affidato e organizza dei piani di sostituzione dello stesso.
In caso di trasferimento in altra struttura, tutte le strumentazioni tecniche restano in uso presso la struttura originaria salvo esplicita autorizzazione congiunta, del dirigente delegato della struttura coinvolta e del Servizio Informativo.

I dispositivi informatici sono strumenti di lavoro appartenenti al patrimonio aziendale e pertanto:

- devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni (i portatili non devono essere lasciati incustoditi, nemmeno provvisoriamente, in luoghi quali uffici aperti, sale riunioni, bauli dell'automezzo in aree di parcheggio e, in caso di utilizzo interno, devono essere riposti, al termine dell'attività lavorativa, in armadi/locali con serratura o assicurati con il cavetto di sicurezza);
- devono essere utilizzati per fini professionali (ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza);
- il verificarsi di alcune azioni quali il furto, il danneggiamento, lo smarrimento, ecc… deve essere prontamente segnalato alle Forze dell'Ordine ed alla Direzione Aziendale. Nel caso in cui si riscontrasse il non rispetto delle regole di conservazione degli strumenti assegnati, potranno essere attivati dall'azienda meccanismi di rimborso del danno subito (bene e attività correlate) e potranno essere applicate sanzioni disciplinari;
- è vietato qualsiasi trattamento inerente contenuti di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- è fatto obbligo all'utente utilizzatore di rimuovere eventuali file elaborati ed utilizzati, prima della riconsegna - particolare attenzione è rivolta nel caso di un utilizzo temporaneo del PC portatile assegnato.

5.2 Credenziali di autenticazione ai dispositivi e alla rete

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente "*userId*", associato ad una parola chiave "*password*" personale e riservata che dovrà venir custodita dall'incaricato con la massima diligenza e non divulgata.
Le credenziali di autenticazione per l'accesso ai dispositivi ed alla rete vengono predisposte dagli amministratori del Servizio Informativo all'atto dell'assunzione del nuovo dipendente in seguito a confacente comunicazione della struttura Politiche e Gestione Risorse Umane e devono essere obbligatoriamente modificate al primo accesso.
La password di accesso alla rete ha un periodo di validità limitato; ad intervalli regolari verrà quindi richiesto all'utente di modificare la password.
In caso di estinzione del rapporto contrattuale con l'Incaricato, la Struttura Politiche e Gestione Risorse Umane, ne dà tempestiva comunicazione, a mezzo posta elettronica, al Servizio Informativo e questi provvede ad inibire l'accesso alle postazioni entro tre giorni lavorativi dal ricevimento della comunicazione (o non appena ne venga a conoscenza).
Qualora la parola chiave dovesse venir sostituita per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, l'utente potrà procedere alla re-inizializzazione della stessa d'intesa con il personale del Servizio Informativo - previo appuntamento e munito di documento di identità in corso di validità.

Per maggiori informazioni e approfondimenti si prega di fare riferimento alla procedura aziendale preposta “gestione delle credenziali e dei profili di accesso”.

5.3 Credenziali di accesso ai servizi e agli applicativi

I dirigenti delegati possono richiedere per i propri collaboratori l'accesso agli applicativi utilizzati in Azienda. Nel caso di collaboratori a progetto e coordinati e continuativi la preventiva richiesta, se necessario, verrà inoltrata direttamente dal dirigente delegato della struttura/ufficio/area con il quale il collaboratore si coordina nell’espletamento del proprio incarico.
Ogni struttura operativa è tenuta ad organizzare e conservare un registro delle credenziali richieste per i propri collaboratori; in tal modo, in caso di sopraggiunta necessità, potrà essere correttamente istanziata la richiesta di disabilitazione degli accessi agli applicativi.
In caso di trasferimento o cessazione del rapporto di lavoro con l'Azienda, inoltre, il dirigente delegato dell’utente in uscita dovrà compilare la modulistica preposta ed inviarla al Servizio Informativo per l'immediata sospensione delle credenziali di accesso agli applicativi gestionali.
Per maggiori informazioni e approfondimenti si prega di fare riferimento alla procedura aziendale preposta “gestione delle credenziali e dei profili di accesso”.

5.4 Caratteristica delle password

Gli incaricati sono responsabili della custodia e dell’utilizzo delle proprie credenziali di autenticazione; la password, formata da lettere (maiuscole e minuscole), numeri e/o caratteri speciali, nei limiti consentiti dai sistemi, deve avere le seguenti caratteristiche:

- deve essere di lunghezza non inferiore ad 8 caratteri oppure, nel caso in cui ciò non sia possibile, da un numero di caratteri pari al massimo consentito dal connesso applicativo;
- deve essere composta da caratteri maiuscoli, caratteri minuscoli, numeri e caratteri speciali (es. Y12s@hT!);
- non deve contenere riferimenti agevolmente riconducibili all’Incaricato o ad ambiti noti;
- deve essere obbligatoriamente cambiata al primo utilizzo e successivamente ogni 90 giorni (per quanto concerne le credenziali di dominio esiste un meccanismo di scadenza automatica);
- deve essere diversa da quella precedentemente utilizzata;
- non deve essere basata su nomi di persone, date di nascita, animali, oggetti o parole ricavabili dal dizionario (anche straniere), o tratta da informazioni personali;
- non deve presentare una sequenza di caratteri identici o in gruppi di caratteri ripetuti;
- non deve essere memorizzata in funzioni di log-in automatico, in un tasto funzionale o nel browser utilizzato per la navigazione Internet;
- deve essere annullata e sostituita con una nuova - per motivate necessità di urgente accesso alle informazioni ed impedimento del titolare delle credenziali - da parte degli amministratori dei servizi o loro delegati. In questo caso essa dovrà essere nuovamente modificata al primo accesso da parte dell’Incaricato.

5.5 Utilizzo delle credenziali

L’utente è tenuto a rispettare i criteri descritti nella sezione CARATTERISTICA DELLE PASSWORD per la creazione/sostituzione di password robuste, anche laddove il software non imponga tale abitudine, e ad eseguire le modifiche periodiche stabilite dall’amministratore di sistema.
L'utente si impegna a non cedere a terzi le proprie credenziali di accesso alla rete, consapevole che la cessione delle stesse consente ad altri l’accesso e l’utilizzo dei relativi servizi, ovvero

l'accesso ai dati cui il soggetto è abilitato con conseguenze quali la visualizzazione di informazioni riservate, la distruzione e/o modifica di dati.
È assolutamente proibito accedere alla rete e ai programmi con delle credenziali di autenticazione, in particolare con un codice d'identificazione utente, diverso da quello assegnato. La responsabilità di qualsiasi azione svolta dopo aver eseguito la procedura di autenticazione sarà attribuita all'utente assegnatario delle credenziali. L'utente è quindi responsabile, sia nei confronti di terzi che dell'Azienda, di fatti e atti illeciti, con particolare riferimento all'immissione in rete di contenuti critici o contrari all'ordine pubblico o al buon costume così come definiti dalla giurisprudenza corrente.
È fatto divieto annotare la password su supporti facilmente rintracciabili e, soprattutto, in prossimità della stazione di lavoro utilizzata.
L'utente si impegna a modificare tempestivamente la password d'accesso alla rete qualora tale dato sia stato rubato, smarrito, perso o sia noto a terzi.
L'Azienda si fa garante della custodia dei dati personali forniti dall'utente e si impegna a non rivelarli a terzi, se non a fronte di legittima richiesta da parte di Autorità Giudiziaria, Autorità di Pubblica Sicurezza e Garante per la Protezione dei Dati Personali.
Nel caso l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia all'Amministratore di sistema ed al Servizio Informativo.
L'Azienda eroga, nell'ambito del Piano di Offerta Formativa, corsi obbligatori riguardanti la Privacy in cui vengono evidenziati, fra gli altri, gli obblighi previsti dalla normativa vigente circa l'assegnazione e la gestione delle credenziali personali di accesso alle risorse informatiche, sistemi ed applicativi software.

5.6 Credenziali amministrative

I privilegi di amministrazione sono limitati ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi previa nomina formale ad "Amministratore di Sistema" (decreto Egas n.71 del 25.07.2017).
A seguito della nomina ad Amministratore viene aggiornato l'inventario delle utenze amministrative contenente gli estremi identificativi delle persone fisiche autorizzate e preposte a tale ruolo.
Laddove il sistema lo permetta, i permessi amministrativi saranno concessi in maniera granulare per consentire unicamente l'evasione delle attività elencate nell'ambito di operatività per cui l'amministratore è stato nominato.
Le password amministrative rivestono particolare rilevanza, pertanto, oltre a quando già indicato nella sezione CARATTERISTICA DELLE PASSWORD, devono essere soggette a maggiori requisiti di complessità.
Le utenze sono di norma nominative e riconducibili ad una sola persona; fanno eccezione le utenze assegnate ad accessi di automi o quelle presenti in particolari contesti che presentano vincoli tali da rendere non supportata la gestione di tali tipologie di utenze. Quest'ultima categoria di sistemi è sottoposta a contromisure di sicurezza compensative, quali l'isolamento su reti distinte, l'interdizione alla navigazione per categorie, la restrizione dell'accesso ad una ridotta white list di URL, o altre sulla base di specifiche valutazioni.
Nelle postazioni client le utenze amministrative locali - le cui password sono comunque conosciute dal solo Servizio Informativo e dal fornitore di servizi Insiel - sono state disattivate o, laddove possibile, rimosse. Le utenze amministrative anonime dei sistemi sono utilizzate solo in situazione di emergenza. Negli altri contesti è in fase di valutazione una modalità che garantisca quanto prescritto.
L'organizzazione aziendale prevede l'assegnazione di credenziali amministrative nominative a più soggetti al fine di garantire l'accessibilità ai dati e agli strumenti elettronici indipendentemente dalla disponibilità dei singoli incaricati.

- Le utenze amministrative devono essere utilizzate dagli amministratori per effettuare le sole operazioni che ne richiedano i privilegi, assicurando così la completa distinzione tra utenze privilegiate e non privilegiate (in alcuni applicativi il login avviene con la medesima credenziale, ma prima dell'effettivo accesso al programma, una particolare procedura permette di selezionare il ruolo che verrà impiegato nell'applicativo per quella particolare sessione operativa).
- In attuazione delle disposizioni dettate dall'Agid con riferimento alle misure minime di sicurezza, l'amministratore di sistema ha l'obbligo di scegliere una password con le seguenti caratteristiche:
    - la lunghezza della password deve essere di almeno 14 caratteri (laddove il sistema non lo permetta, 8 caratteri o la maggiore supportata);
    - la password deve soddisfare adeguati requisiti di complessità: non deve contenere parti del nome utente, deve includere lettere maiuscole, lettere minuscole, numeri e caratteri non alfanumerici (ad es. !, $, #, %, ecc.)
    - le password delle utenze amministrative devono essere sostituite con frequenza non superiore a 90 giorni (password aging)
    - le password già utilizzate non devono essere riutilizzate a breve distanza di tempo, è fatto obbligo di non riutilizzare vecchie password prima di 10 modifiche (password history).

5.7 Utilizzo del personal computer e del laptop

Il personal computer dato in affidamento all'utente/servizio permette l'accesso alla rete di Egas solo attraverso specifiche credenziali di autenticazione, come meglio descritto nella sezione "CREDENZIALI DI AUTENTICAZIONE" della presente Policy.
Tutti i PC portatili devono collegarsi periodicamente, con frequenza almeno mensile, alla rete interna per consentire l'aggiornamento dell'antivirus, del sistema operativo e del software.
A meno di preventiva e formale autorizzazione del Servizio Informativo, che verrà rilasciata solo per comprovate esigenze operative, il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici (tale comportamento risulta indispensabile per la corretta conservazione dei beni, per prevenire possibili problemi di sicurezza fisica e logica e per permettere l'inoculamento remoto di idonee policy).
Qualora, per motivate ragioni di efficienza ed efficacia, un incaricato venga abilitato all'utilizzo della propria postazione con il ruolo di amministratore locale, è comunque tenuto a rispettare il presente regolamento - a titolo puramente esemplificativo e non esaustivo si ribadisce che è assolutamente vietata l'installazione di qualsiasi tipologia di applicazione senza preventiva formale autorizzazione del Servizio Informativo.
Le unità di memorizzazione locali (ad esempio il disco rigido della propria postazione di lavoro), non sono soggette al salvataggio.

- Non è consentito all'utente modificare le caratteristiche hardware e software del PC, inclusa la configurazione di rete (eccezione fatta per la sola modifica alle impostazioni di rete dei dispositivi portatili che manifestano ingenti esigenze di mobilità).
- Non è consentita l'attivazione in autonomia della password di accensione (bios), senza preventiva autorizzazione da parte del Servizio Informativo.
- Non è consentito all'utente procedere all'installazione di dispositivi di memorizzazione, comunicazione o altro (es. masterizzatori, modem, etc.) in assenza di preventiva autorizzazione del Servizio Informativo.
- Non è consentito lo spostamento del PC e delle relative periferiche senza preventiva esplicita autorizzazione del Servizio Informativo.

- Qualora l'utente sia costretto ad assentarsi dal locale in cui è ubicata la stazione di lavoro o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima è tenuto ad eseguire una delle seguenti operazioni: spegnimento, blocco o disconnessione dalla sessione di lavoro (lasciare un elaboratore incustodito e connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso); in Egas è stata implementata una policy che prevede il blocco automatico della postazione dopo alcuni minuti di inattività.
- Non è consentita la copia di file da supporti di memorizzazione esterni, come pure il download di file dalla rete, i cui contenuti non abbiano attinenza con la prestazione lavorativa.
- Non è consentito il salvataggio di dati, in particolare se attinenti alle "categorie particolari" secondo il Regolamento UE 2016/679, nei supporti di memorizzazione locali dei computer se non per esigenze estemporanee; l'Azienda non è responsabile dell'integrità dei dati localmente archiviati.
- I dati attinenti alle "categorie particolari" secondo il Regolamento UE 2016/679, non possono essere trattati nei supporti di memorizzazione locali dei computer a meno di utilizzo di adeguati sistemi di protezione crittografica.

5.8 Utilizzo e conservazione dei supporti rimovibili

I supporti rimovibili (CD e DVD anche riscrivibili, supporti USB, hard disk ecc.) devono essere limitati a quelli strettamente indispensabili alle attività aziendali; in tali supporti non devono essere conservati, nemmeno provvisoriamente, file aziendali congiuntamente a file personali.

- L'utente assegnatario è responsabile della custodia dei supporti e dei dati in essi contenuti.
- I supporti rimovibili contenenti attinenti alle "categorie particolari" secondo il Regolamento UE 2016/679, nonché informazioni costituenti il know-how aziendale devono essere ridotti ai casi di assoluta ed estemporanea necessità e devono essere cifrati con password di adeguata robustezza; tali dispositivi devono essere custoditi dagli utenti con le medesime modalità imposte per la documentazione cartacea contenente la stessa tipologia di informazioni. Qualora non più utilizzati, devono essere distrutti o resi inutilizzabili.
- Non è consentito l'utilizzo dispositivi esterni di dubbia provenienza; ogni dispositivo di memorizzazione di provenienza esterna all'Ente dovrà essere verificato mediante il programma antivirus prima del suo utilizzo (consultare sezione ANTIMALWARE).
- I supporti rimovibili devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato e/o alterato e/o distrutto, o, successivamente alla cancellazione, recuperato. Al fine di assicurare la distruzione e/o inutilizzabilità di supporti rimovibili, ciascun utente dovrà utilizzare gli strumenti messi a disposizione dal sistema operativo in uso per procedere alla formattazione a basso livello del supporto.

5.9 Unità di rete, memorizzazione file e backup

Le unità e le cartelle di rete sono le rappresentazioni dello storage aziendale.
Gli utenti del dominio Aziendale possono utilizzare, previa richiesta del proprio dirigente delegato, un sistema di salvataggio dei file sul quale vengono svolte regolari attività di controllo e amministrazione.
Insiel S.p.A. gestisce lo storage aziendale; i dati conservati in tali aree sono protetti da procedure di backup automatico gestite e monitorate dal concessionario stesso; la policy attuale è configurata per un backup incrementale giornaliero e un'archiviazione full mensile con

profondità 1 anno. Il backup incrementale salva i dati inseriti o modificati rispetto all'ultimo backup incrementale eseguito; qualora un file venisse cancellato, può essere ripristinato dai salvataggi per 60 giorni (per poi essere rimosso). Ogni mese viene fatta un'archiviazione completa dei dati, una sorta di fotografia dei dati presenti in quel momento. Questo salvataggio viene mantenuto nei backup per 1 anno. Alla fine dell'anno il salvataggio viene cancellato.
Le copie di backup sono memorizzate di norma su supporti/sistemi custoditi fisicamente in locali ad accesso controllato in completa gestione del fornitore ed almeno una copia di backup viene memorizzata su supporti/sistemi distinti logicamente o fisicamente e non direttamente accessibili al sistema stesso (Insiel).
Costituisce buona regola la pulizia periodica (almeno ogni sei mesi) degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È assolutamente da evitare un'archiviazione ridondante.

- Le cartelle di rete presenti negli storage sono aree di condivisione di informazioni strettamente professionali e non devono in alcun modo essere utilizzate per scopi diversi; qualunque file non legato all'attività lavorativa non può essere dislocato, nemmeno temporaneamente, in queste unità. Il personale del Servizio Informativo, senza necessità di esplicita autorizzazione, si riserva la facoltà di procedere alla verifica ed eventuale rimozione di qualsiasi file memorizzato nelle cartelle di rete qualora ritenuto pericoloso per la sicurezza o non attinente all'attività lavorativa.
- I privilegi di lettura e scrittura delle cartelle vengono definiti dal dirigente delegato valutando il bilanciamento delle esigenze della produttività e della necessaria riservatezza.
- Non è consentita la modifica dei permessi di accesso delle cartelle di rete da parte degli utenti.
- Per il ripristino dei dati accidentalmente persi o modificati sulle cartelle di rete è fatto obbligo di avvisare tempestivamente il Servizio Informativo.
- Ove possibile, il Servizio Informativo metterà a disposizione degli utenti che ne facessero richiesta, per il tramite del proprio dirigente delegato, una cartella di rete. L'utente potrà utilizzare in maniera esclusiva e riservata tale unità per il solo salvataggio dei dati di natura strettamente aziendale.

Alla data di conclusione del rapporto di lavoro la struttura Politiche e Gestione Risorse Umane notificherà l'interruzione del rapporto di lavoro al Servizio Informativo indicandone la tipologia (cessazione o sospensione). Salvo diverse indicazioni, specifiche richieste e casi particolari che verranno opportunamente trattati, entro 3gg dal ricevimento della comunicazione, il Servizio Informativo procederà alla variazione dei permessi della cartella di rete concessa in maniera esclusiva (qualora richiesta) affinché sia consentito al dirigente delegato, o altra figura delegata, di effettuare l'accesso ai file contenuti per l'esecuzione di eventuali backup.
Per i soli di casi di cessazione del rapporto di lavoro (mobilità in uscita, pensionamento, dimissioni o decesso), trascorsi ulteriori 60 giorni, periodo stimato pertinente e non eccedente a garantire l'operatività e la continuità di servizio, salvo diverse indicazioni degli assegnatari o dei responsabili, specifiche richieste e casi particolari che verranno opportunamente trattati, il Servizio Informativo procederà alla cancellazione definitiva della cartella di rete assegnata in modalità esclusiva e non sarà possibile recuperare i dati in essa contenuti.

5.10 Archivi con particolari requisiti di riservatezza

- Ogni file afferente alle "categorie particolari" secondo il Regolamento UE 2016/679 dovrà essere protetto con modalità idonee a impedire l'illecita o fortuita acquisizione delle informazioni da parte di soggetti diversi da quelli autorizzati.

- I dati archiviati, in particolare quelli afferenti alle "categorie particolari" secondo il Regolamento UE 2016/679 possono essere conservati per un periodo non superiore a quello necessario per adempiere agli obblighi o ai compiti istituzionali.
- Nell'invio di dati afferenti alle "categorie particolari" secondo il Regolamento UE 2016/679 tramite posta elettronica, la spedizione del file deve avvenire in forma di allegato e non come testo del messaggio. Il file allegato dovrà essere protetto con modalità idonee a impedire l'illecita o fortuita acquisizione da parte di soggetti diversi dal destinatario che potrà consistere in una password per l'apertura del file o in una chiave crittografica rese note agli interessati attraverso separata comunicazione (come richiesto dalla vigente normativa).

5.11 Utilizzo carte operatore (firma digitale)

I dirigenti delegati possono richiedere, per motivate esigenze operative, il rilascio di carte operatore per i propri collaboratori.
Le carte operatore, dotate di un certificato di autenticazione e di un certificato di firma digitale, vengono utilizzate come sistema di sicurezza informatico allo scopo di accedere a servizi o consentire a un documento elettronico di avere validità legale al pari di un testo autografato a mano. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi ne dia prova contraria.
La generazione e l'emissione di una nuova carta operatore richiedere un tempo variabile da 2 a 6 mesi (Insiel S.p.a.). Per i casi di urgenza è possibile richiede una carta temporanea, denominata "carta jolly"; nelle carte prodotte dal 03.02.2018, la durata massima del certificato di firma è stata estesa da 3 a 12 mesi e la durata del certificato di autenticazione da 3 a 24 mesi. Alla scadenza dei termini indicati la carta jolly deve venir ri-emessa poiché il certificato risulterebbe scaduto di validità.
Per evitare disservizi legati alla scadenza dei certificati è onere del titolare contattare il Servizio Informativo 120 giorni prima della scadenza riportata sulla carta, al fine di compilare e sottoscrivere per tempo la documentazione necessaria alla nuova emissione.
È obbligo del titolare:

- utilizzare personalmente il dispositivo di firma;
- custodire i codici di accesso (PIN e PUK) e non comunicarli a nessuno;
- (solo per carte "jolly") al primo utilizzo - o in collaborazione al Servizio Informativo durante la consegna del dispositivo - modificare il PIN pre-impostato;
- assicurare la custodia del dispositivo di firma (carta operatore) o degli strumenti di autenticazione informatica per l'utilizzo del dispositivo di firma da remoto, e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri

5.12 Utilizzo dispositivi personali

- Per ragioni di sicurezza è fatto divieto di connettere alla rete LAN e alla rete WLAN aziendale (eccezione fatta per la WLAN "egas-ospiti") dispositivi personali se non su esplicita e formale autorizzazione del Servizio Informativo. In tale contesto, per "dispositivi personali" si intendono tutti i dispositivi - a titolo puramente esemplificativo e non esaustivo, laptop, stazioni di lavoro, tablet, cellulari, sistemi di connessione - la cui pertinenza non sia riconducibile all'Egas o il cui utilizzo sia esclusivo all'erogazione di servizi contrattualizzati per l'Egas stessa.

5.13 Utilizzo di stampanti, multifunzioni e fax-server

- È vietato l'utilizzo delle stampanti, delle fotocopiatrici (MF) e dei Fax aziendali per fini personali.
- Il materiale stampato deve essere immediatamente prelevato per evitare che possa essere visionato da personale non autorizzato.
- La stampa di documenti informatici dovrà essere limitata ai casi per cui esiste l'assoluta necessità di disporre della copia cartacea.
- Nella trasmissione di documenti tra le pubbliche amministrazioni è vietato l'utilizzo del Fax o del FaxServer (d.lgs. 82/2005 e ss.mm.ii: l'inosservanza della disposizione, ferma restando l'eventuale responsabilità per danno erariale, comporta responsabilità dirigenziale e responsabilità disciplinare).
- Nelle stampanti multifunzione (MF), la scansione dei documenti potrebbe venir configurata come "scan-to-mail" - invio del documento digitalizzato ad una casella di posta - e/o "scan-to-disk" - salvataggio delle scansioni su una cartella locale della multifunzione o su cartella di rete.
- Nell'utilizzo in modalità "scan-to-mail" è proibito l'invio di scansioni dalla multifunzione verso e-mail non aziendali. Qualora si desideri inviare una scansione ad un soggetto terzo afferente all'Ente, è necessario dapprima inoltrare il documento alla propria e-mail istituzionale – per verificarne il contenuto - e solo successivamente, utilizzando la propria cassetta e-mail, inoltrare l'allegato al destinatario. Nel caso di invio di allegati pesanti è opportuno, dopo aver salvato la scansione, cancellare la mail dalla posta in arrivo e, successivamente, dal cestino.
- La modalità "scan-to-disk" potrebbe indirizzare i documenti acquisiti nella memoria interna del dispositivo, oppure in una share di rete. In entrambi i casi, al fine di preservare lo storage ed evitare il blocco del dispositivo per insufficienza di spazio, potrebbero essere impostate delle policy che eliminano i documenti più vecchi di 24h. In seguito all'eliminazione non sarà possibile procedere al recupero degli stessi. La cancellazione periodica non dispensa l'utente dall'obbligo di cancellare/spostare le scansioni eseguite dalla cartella condivisa nel più breve tempo possibile (al fine di non rendere noto a terzi il contenuto dei file acquisiti).

5.14 Configurazione di sistema

Per ciascuna tipologia di ambito aziendale vengono definite configurazioni standard che sono applicate sistematicamente e gestite centralmente per garantire adeguati livelli di sicurezza.
Tutte le postazioni di lavoro, prima di essere assegnate, verranno pertanto clonate utilizzando master disk appositamente realizzati per le specifiche necessità dell'Ente e saranno aderenti alle misure minime di sicurezza ICT per le pubbliche amministrazioni.
La memorizzazione delle immagini di installazione avviene offline rispetto al contesto elaborativo degli specifici sistemi a cui le immagini si riferiscono (ad esempio disco esterno).
Tutte le macchine vengono connesse al dominio attraverso un'operazione di "join" e legate al distributore antivirus dedicato alle postazioni di lavoro dell'Ente.
Alla data di pubblicazione del presente documento, in Azienda è attiva una configurazione basata su Dominio Microsoft Windows 2012 e Active Directory. Sono stati installati due Domain Controller distribuiti sul territorio.
Tutti i Personal Computer aziendali devono essere collegati alla rete dati affinché siano protetti da minacce esterne (worm, trojanhorse, ecc..) e ricevano nuove GPO; non possono per nessun motivo essere scollegati da tale rete. Casi particolari in cui il computer non debba essere connesso alla rete aziendale devono essere esplicitamente autorizzati dal Servizio Informativo.
Qualora i sistemi in esercizio vengano compromessi, è previsto il ripristino degli stessi con l'utilizzo di configurazioni standard (master disk).

- Non è consentito modificare in alcun modo le configurazioni impostate sulle risorse aziendali.

Per peculiari necessità operative, alcune postazioni, strettamente destinate alla gestione delle emergenze, sono fornite e gestite da INSIEL spa che ne cura direttamente la configurazione dell'hardware dedicato in relazione all'ottimizzazione della qualità dei servizi ed alla necessità di effettuare frequenti connessioni e disconnessioni del personale coinvolto.

5.15 Hardware

L'hardware potrà essere acquistato solo previa autorizzazione del Servizio Informativo che controllerà le richieste al fine di valutarne la compatibilità con i sistemi in uso e l'infrastruttura di rete.
Le richieste di acquisto dell'hardware dovranno essere motivate, sottoscritte dal Dirigente delegato di struttura/ufficio/area, ed indirizzate al responsabile dei Servizi Informativi ed al responsabile del Provveditorato Centralizzato.
Il Servizio Informativo si riserva la facoltà di bloccare in qualsiasi momento le interfacce USB delle stazioni di lavoro per impedire l'utilizzo di supporti di massa rimovibili (principale ingresso di codice malevole).

- È fatto assoluto divieto all'utente di intervenire in qualunque modo sull'hardware in dotazione. In caso di malfunzionamento delle apparecchiature assegnate, l'utente si impegna a darne tempestiva segnalazione al Contact Center Insiel S.p.A., - RICHIESTA DI ASSISTENZA TECNICA (HELP DESK).
- Non è consentito l'utilizzo di hardware di tipo personale salvo specifica autorizzazione del Servizio Informativo.
- Non è consentita l'installazione autonoma di alcun dispositivo di memorizzazione, comunicazione o altro - per quanto attinente ai dispositivi esterni consultare la sezione "UTILIZZO E CONSERVAZIONE DEI SUPPORTI RIMOVIBILI".

5.16 Software

Tutti i software utilizzati all'interno dell'Ente devono essere regolarmente licenziati.
Nuove necessità rigorosamente legate ad esigenze lavorative andranno pertanto presentate al Servizio Informativo come descritto nella procedura "POLICY EGAS PER L'INSTALLAZIONE DI NUOVO SOFTWARE"; il nuovo software acquisito dovrà venire registrato a nome dell'Ente.
Nell'ipotesi di utilizzo di software realizzato direttamente dall'utente finale sarà necessario darne comunicazione al Servizio Informativo e, qualora vengano trattati "categorie particolari" secondo il Regolamento UE 2016/679, ricevere formale autorizzazione al trattamento dei dati dal Titolare dei dati.
Sono in uso particolari software - alla data di pubblicazione del presente documento "CA" - volti a fornire, con cadenza programmata (attualmente, la pianificazione è settimanale) report specifici in merito ai software installati nelle postazioni di lavoro.
Su tali report sono effettuate attività di analisi volte a rilevare la presenza di software non autorizzato.

- Non è consentito l'utilizzo di programmi diversi da quelli ufficialmente installati dai tecnici dal Servizio Informativo (o dall'Insiel S.p.A. per conto del Servizio Informativo) o resi disponibili in ambito SISSR o in ambito ministeriale. Al fine di proteggere l'integrità dell'Azienda, il personale non può utilizzare software di proprietà personale. Tutto ciò comprende anche le applicazioni regolarmente acquistate e registrate, programmi

shareware e/o freeware, eventuale software scaricato da Internet o proveniente da CD/DVD allegati a riviste e/o giornali o altro software posseduto a qualsiasi titolo.

- È fatto divieto a chiunque utilizzi computer aziendali di scaricare dalla rete Internet o installare qualsiasi tipo di software non autorizzato (sussistendo il grave pericolo di introdurre codice malevolo e/o di alterare la funzionalità delle applicazioni software esistenti).
- Non è consentita la riproduzione o la duplicazione di programmi informatici ai sensi della Legge n. 128 del 21.05.2004.
- Non è consentita l'installazione, anche se necessaria, di eventuali driver per stampanti o altri supporti (come ad esempio masterizzatori, scanner, etc.); in questo caso l'utente dovrà richiedere ai tecnici del Servizio Informativo di intervenire per effettuare l'installazione.
- Non è consentita la disinstallazione dei programmi, sia software di base che software applicativi. I suddetti interventi sono effettuati, in caso di necessità, solo a cura dei tecnici del Servizio Informativo - o da Insiel S.p.A. per conto del Servizio Informativo - funzionalmente alle segnalazioni dell'utenza.

5.17 Aggiornamenti software e correzione delle vulnerabilità

Gli aggiornamenti del sistema operativo sono necessari, oltre che essere un obbligo di legge, al fine di proteggere i PC e l'intera rete.
In collaborazione con Insiel S.p.A., che governa il servizio, è stato attivato il Windows Server Update Services (WSUS) che pianifica e dispone l'installazione degli aggiornamenti in modalità automatica.
Sempre in collaborazione con Insiel, che amministra il servizio, è stato installato un Server per la gestione Antivirus. Tutte le postazioni vengono associate a tale istanza che - legata in modo diretto con il produttore (alla data di pubblicazione del presente documento "Trend Micro") - distribuisce prontamente eventuali aggiornamenti di pattern, antivirus e antispyware. Nelle postazioni eventualmente off-line tali aggiornamenti vengono installati non appena si ripresenteranno in linea, di norma, alla prima accensione. Tale modalità permette di elevare al massimo la protezione contro virus ed agenti esterni.
Per quanto concerne l'esecuzione dei controlli di vulnerabilità sui sistemi in rete, l'Egas utilizza un'infrastruttura dedicata - alla data di pubblicazione del esente documento, "Nessus Professional 7.0.0" – regolarmente aggiornata con tutte le più rilevanti vulnerabilità di sicurezza, sulla quale sono state configurate delle scansioni pianificate.
È stata inoltre realizzata la "PROCEDURA PER LA GESTIONE DELLE VULNERABILITÀ", il cui scopo è quello di verificare che le vulnerabilità emerse vengano correttamente gestite (anche attraverso un regolare riesame di accettazione dei rischi) attuando opportune azioni in funzione alla priorità della vulnerabilità riscontrata,

- È tassativamente vietato all'utente ogni sorta di aggiornamento manuale del software installato se non espressamente autorizzato dal Servizio Informativo. Gli aggiornamenti del software e dei driver necessari al buon funzionamento della postazione di lavoro saranno effettuati direttamente dai tecnici del Servizio Informativo (o da Insiel S.p.A. per conto del Servizio Informativo) configurando gli aggiornamenti automatici per ciò che attiene la protezione antivirus ed il sistema operativo, ed intervenendo dietro segnalazione dell'utente per ogni ulteriore update si dovesse rendere necessario.

5.18 Utilizzo della rete fisica (LAN)

La rete fisica (LAN – Local Area Network) si basa sul protocollo TCP/IP ed è una risorsa strategica per l'Azienda in quanto connette ogni dispositivo informatico veicolando i dati

conservati negli archivi centrali. Funge da mezzo di trasporto per altri tipi di informazioni, pertanto, ogni disservizio o sua interruzione, comporta notevoli disagi per l'operatività dell'Azienda medesima. Tutte le postazioni di lavoro operano interconnesse alla rete aziendale e possono così accedere ai dati secondo precise abilitazioni. Nello specifico, la configurazione e la gestione di tutti gli apparati attivi e dell'infrastruttura di collegamento sono affidati al concessionario Insiel S.p.A.

- Non è consentita la connessione alla rete aziendale di apparati atti ad effettuare connessioni con altre reti verso l'esterno (router, bridge, modem, impianti wireless, ecc.). Un eventuale uso di tali apparati, qualora necessario, dovrà essere richiesto al Servizio Informativo e ricevere autorizzazione dalle Direzioni competenti. Analogamente non è ammesso, se non per esigenze estemporanee e previa autorizzazione del Servizio Informativo, l'utilizzo non autorizzato di dispositivi per lo sdoppiamento di punti rete (mini Hub).
- Viene fatto esplicito e tassativo divieto di connettere in rete stazioni di lavoro ed ogni altro dispositivo informatico (es. computer e portatili non aziendali) se non previa esplicita e formale autorizzazione Servizio Informativo. Introdurre una macchina con un IP duplicato potrebbe causare un conflitto con l'indirizzo di un server oppure di un altro dispositivo della rete stessa e causare gravi malfunzionamenti alla rete.
- È fatto assoluto divieto di configurare servizi già messi a disposizione in modo centralizzato, quali ad esempio, e non solo, DNS (Domain Name Service), DHCP (Dynamic Host Configuration Protocol), NTP (Network Time Protocol), mailing, accesso remoto, proxy server.
- È fatto assoluto divieto all'utente di intercettare ed analizzare i pacchetti sulla rete aziendale, utilizzando analizzatori di rete sia software che hardware. L'utilizzo di tali strumenti è strettamente riservato al personale tecnico del Servizio Informativo al fine di monitorare le prestazioni della rete aziendale.
- Nel caso si riscontrasse la presenza di PC che generano traffico anomalo o che potrebbero far diminuire le prestazioni dell'intero sistema, sarà facoltà del personale del Servizio Informativo procedere al blocco, se necessario, dell'attività di rete della postazione.
- È fatto divieto di svolgere attività intenzionali che portino in qualunque modo alla saturazione dei sistemi di elaborazione e di trasmissione dati, rendendo anche temporaneamente indisponibili risorse di uso comune agli utenti.
- Non è consentito l'accesso agli armadi di rete, la modifica delle connessioni o la manomissione di qualunque impianto o cavo vi sia contenuto. Non è consentito depositare materiale nelle vicinanze degli armadi di rete e nel raggio d'azione della porta di accesso all'armadio.
- È obbligatorio interpellare il Servizio Informativo prima di ogni spostamento di postazioni informatiche, per valutarne l'impatto e la fattibilità e per predisporre le adeguate configurazioni.

5.19 Utilizzo della rete Wireless (WLAN)

Ad integrazione della rete LAN descritta nella precedente sezione "UTILIZZO DELLA RETE FISICA (LAN)", alcune aree dell'Egas sono servite da reti senza fili, Wireless LAN, per consentire la trasmissione dei dati attraverso canali senza fili.
Utilizzando apparati Access Point vengono distribuiti due SSID (service set identifier – nome con cui una rete senza fili si identifica ai suoi utenti), "egas-ospiti" ed "egas-enterprise" secondo specifiche esigenze.

La WiFi-LAN “egas-enterprise” risulta a tutti gli effetti un’estensione della rete LAN, pertanto, i client connessi, avranno la possibilità di accedere alle medesime risorse della rete locale cablata.
I dirigenti delegati possono chiedere, per motivate esigenze di mobilità, per i propri collaboratori che utilizzano laptop di proprietà Egas, l’accessibilità all’infrastruttura “egas-enterprise”.
La tecnologia è configurata e governata da Insiel S.p.A., Egas dispone il rilascio delle abilitazioni per il tramite del Servizio Informativo funzionalmente alle richieste inviate dai dirigenti delegati.

- è fatto divieto assoluto al personale abilitato alla rete WLAN “egas-enterprise” di connettersi a tale infrastruttura utilizzando sistemi diversi dai dispositivi aziendali quali portatili e tablet preventivamente configurati dal Servizio Informativo (per esempio, è fatto divieto di accesso per mezzo di cellulari, oppure laptop e tablet di tipo personale).

5.20 Accesso ad applicazioni e banche dati

In relazione all'utilizzo delle risorse informatiche aziendali, nonché di quelle messe a disposizione dal Sistema Informativo Socio Sanitario Regionale (SISSR), il Servizio Informativo fornisce le credenziali di accesso ai singoli operatori in coerenza alle richieste pervenute dai dirigenti delegati. È obbligo dei dirigenti delegati medesimi comunicare prontamente qualsiasi modifica relativa all'organico in carico che richieda la sospensione e/o la revoca dell'autorizzazione all'accesso alle risorse informatiche e alle banche dati**.**

5.21 Antimalware

L’Egas utilizza il servizio Antivirus erogato da Insiel S.p.A.
La politica di sicurezza aziendale prevede l’installazione di un software antimalware (antivirus) su tutte le postazioni di lavoro (che lo supportano); esso viene aggiornato automaticamente grazie ad una gestione centralizzata per mezzo di un server dedicato. Non è ammesso l'utilizzo di sistemi antivirus diversi, se non espressamente formalizzato dal Servizio Informativo. Tra le funzionalità del software antimalware presente su tutti personal computer aziendali vi sono anche funzionalità specifiche di firewalling.
L’esecuzione automatica dei contenuti dinamici presenti nei file, l’apertura automatica dei messaggi di posta elettronica, come pure l’anteprima automatica dei contenuti dei file sono state disabilitate utilizzando adeguate configurazioni sul dominio aziendale.
È stata inoltre abilitata di default su tutti i client la modalità “*Scan all files in removable storage devices after plugin*” atta ad effettuare la scansione di tutte le periferiche rimovibili che vengono collegate. È inoltre attivo il blocco dell’esecuzione “autorun” che disinnesca l’esecuzione automatica di contenuti al momento della connessione dei dispositivi mobili.
Tramite la piattaforma antimalware - attiva a livello regionale - vengono filtrati i messaggi di posta in funzione al loro contenuto prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam; alcuni file (la cui tipologia è considerata non strettamente necessaria o pericolosa) vengono bloccati nella posta elettronica e nel traffico web.

- Ogni dispositivo di memorizzazione esterno deve essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus non eliminabile dal software, non dovrà essere utilizzato, bensì immediatamente scollegato.

Ogni utente è tenuto a controllare la presenza del software antivirus verificandone la presenza dell’icona sulla systray (zona in basso a destra del desktop) del proprio sistema operativo;

nell'eventualità si ravvisasse la mancanza di tale software l'utente dovrà darne immediata segnalazione al Servizio Informativo per attivare le successive azioni inerenti l'installazione.
Nel caso il software antivirus rilevi la presenza di un virus che non è riuscito a ripulire, l'utente dovrà immediatamente:

- sospendere ogni elaborazione in corso senza spegnere il computer;
- segnalare l'accaduto all'HelpDesk Insiel (consultare la sezione "RICHIESTA DI ASSISTENZA TECNICA (HELP DESK)");

5.22 Controllo remoto per manutenzioni IT e accesso degli utenti esterni

Per facilitare e rendere maggiormente tempestive le operazioni di aggiornamento del software e per garantire la sicurezza dei dispositivi, delle applicazioni e dei dati, i tecnici informatici possono avvalersi di strumenti di controllo remoto che consentano di compiere le necessarie operazioni attraverso la rete locale o un collegamento protetto.
La connessione da e verso i sistemi indicati avviene attraverso protocolli dotati di meccanismi che garantiscono nativamente sicurezza o protezione della connessione stessa (ad es. RDP, SSH e https) o attraverso l'utilizzo di canali sicuri o reti interne.
Eventuali specifiche situazioni di impossibilità di utilizzo del protocollo crittografato sono gestite puntualmente attraverso una valutazione del rischio.
Sui dispositivi informatici aziendali è di norma installato un componente di accesso remoto - alla data di pubblicazione del presente documento "CA", conforme alle misure di sicurezza - configurato in modo che l'Utente sia consapevole e debba approvare l'intervento del personale tecnico accettandone la connessione. La durata del collegamento è limitata al tempo strettamente necessario per l'esecuzione e la verifica dell'intervento effettuato.
L'Amministratore del Sistema, per l'espletamento delle sue funzioni (ad esempio il salvataggio e il ripristino degli archivi, la tutela della sicurezza informatica, ecc.) ha la facoltà di accedere, nel rispetto della normativa vigente, ai dati trattati da ciascun utente - ivi compresi gli archivi di posta elettronica. L'Amministratore del Sistema può altresì, in qualunque momento, procedere alla rimozione di file o applicazioni che riterrà essere pericolosi per la sicurezza.
Le ditte che effettuano manutenzioni da remoto agli applicativi o ai server, accedono come utenti esterni alla rete aziendale attraverso un accesso VPN (Virtual Private Network) protetto da Firewall gestito da Insiel S.p.A.
L'abilitazione e le credenziali di accesso vengono forniti dal personale del Servizio Informativo - che inoltra apposita richiesta ad Insiel S.pa. per il seguito di competenza - successivamente alla presentazione della modulistica preposta. Le utenze sono nominali ed inserite sull'albero di Active Directory Egas in unità organizzative preposte.

5.23 Internet e navigazione

Il PC in uso all'utente, qualora abilitato alla navigazione in Internet, costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa.
L'abilitazione alla navigazione è assegnata a livello di utenza e deve essere autorizzata dal Dirigente delegato che istanzia opportuna richiesta al Servizio Informativo.
È attivo un sistema di protezione della navigazione Internet che prevede il filtraggio del traffico per categorie di contenuti ed è inoltre presente la funzionalità di gestione di specifiche blacklist di url.
Sono vietate in modo tassativo le seguenti attività.

- È assolutamente vietato l'utilizzo di credenziali di accesso ad Internet diverse da quelle di cui si è assegnatari.
- Non è consentito l'utilizzo di modem per il collegamento alla rete.

- Non è consentita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.
- Non è consentito il download/upload di software e/o contenuti non autorizzati o comunque non legati all'attività lavorativa.
- Non è consentito l'utilizzo dei servizi di messaggistica istantanea (esclusi quelli espressamente autorizzati dall'azienda); programmi di condivisione file (file sharing); di programmi P2P.
- Non è consentita la registrazione e la partecipazione a Forum non professionali, l'utilizzo di chat line, di social networks, e bacheche elettroniche - esclusi quelli espressamente autorizzati dall'azienda.
- Non è consentito l'utilizzo di qualsiasi software che consenta l'accesso alla postazione di lavoro - controllo remoto - o ai dati istituzionali al di fuori della rete aziendale (condivisione dati online).
- Non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dalla Direzione Aziendale.
- Non è consentita alcuna attività legata ad operazioni di hackeraggio e pirateria informatica in generale.

È responsabilità dell'utente qualsiasi danno arrecato all'Azienda nell'utilizzo della connessione ad Intenet in termini di sicurezza o illecito. L'utente è direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l'uso fatto del servizio Internet. La responsabilità si estende anche alla violazione degli accessi protetti, del copyright e delle licenze d'uso.

5.24 Posta elettronica ordinaria (PEO)

Al momento dell'assunzione, il personale afferente all'EGAS viene dotato di credenziali di accesso alle postazioni e di indirizzo di posta elettronica ordinaria istituzionale (PEO). La PEO può essere rilasciata "ad personam", associata ad una AOO, associata ad un ufficio o associata ad una specifica funzione/progetto o servizio.
La casella di posta elettronica assegnata all'utente è uno strumento di lavoro di proprietà aziendale concesso in uso al lavoratore al fine di un più proficuo svolgimento della prestazione.
Le *caselle di posta nominative*, vengono assegnate utilizzando il seguente formato: nome.cognome@egas.sanita.fvg.it - in caso di omonimia verrà aggiunto un progressivo numerico: nome.cognome2@egas.sanita.fvg.it, nome.cognome3@egas.sanita.fvg.it, ecc.
Possono essere assegnate, qualora si rendesse necessario per esigenze organizzative del lavoro e dietro richiesta del dirigente delegato, delle caselle di posta del tipo: servizio.informativo@egas.sanita.fvg.it. Questa tipologia di *caselle di posta di servizio non personali* verrà utilizzata per un più rapido scambio delle comunicazioni interne e dovrà essere consultata con frequenza giornaliera. Sarà cura del dirigente delegato della struttura interessata verificare l'esistenza di tale casella e, in caso negativo, farne richiesta al Servizio Informativo. In tale richiesta dovranno essere elencati i nominativi e le modalità di accesso delle persone autorizzate, le finalità di utilizzo e se l'indirizzo dovrà essere pubblicato sul sito web istituzionale e sulla rubrica aziendale.
La posta elettronica è controllata da una piattaforma Microsoft Exchange con autenticazione integrata ad Active Directory; la piattaforma, a livello regionale, è governata da Insiel S.p.A.
L'accesso alla casella di posta elettronica aziendale (https://posta.um.fvg.it/owa/) avviene attraverso un codice di identificazione personale e una parola chiave segreta. Alla data di pubblicazione del presente documento dette credenziali coincidono con quelle di accesso alla postazione di lavoro ("egasad\nome.cognome" e "password") e sono modificabili dall'utente assegnatario in totale autonomia.

Anche l'accesso alla mail di servizio non personale, se autorizzato, avviene con le credenziali personali; ad esempio, qualora si volesse effettuare l'accesso alla casella servizio.informativo@egas.sanita.fvg.it
sarà necessario connettersi all'indirizzo
http://posta.um.fvg.it/OWA/servizio.informativo@egas.sanita.fvg.it
ed accedere con le proprie credenziali personali come indicato al paragrafo precedente.
Seguendo le precedenti indicazioni, l'utente potrà consultare tutte le cassette postali a cui è stato autorizzato direttamente da web; tale soluzione offre pertanto la possibilità di accedere alla propria cassetta postale anche al di fuori dell'ambiente lavorativo.
È possibile ottenere, nelle comunicazioni esterne ed interne all'azienda, una segnalazione relativamente al recapito del messaggio e all'avvenuta lettura; si ricorda tuttavia che la conferma di avvenuta lettura è a discrezione del destinatario. Per avere garanzia i quanto sopra è opportuno chiedere al destinatario di confermare esplicitamente o utilizzare gli strumenti preposti "POSTA ELETTRONICA CERTIFICATA (PEC)".
Al fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l'accesso ai dati nel rispetto del principio di necessità e di proporzionalità, il sistema, in caso di assenze programmate, invierà automaticamente messaggi di risposta contenenti le coordinate di posta elettronica di un altro soggetto o altre modalità utili di contatto della struttura. In tal caso, la funzionalità deve essere attivata manualmente dall'utente che dovrà accedere alla Webmail OWA (come descritto nei paragrafi precedenti) ed impostare il messaggio in risposta a tutti i messaggi ricevuti:
opzioni → tutte le opzioni → organizza posta elettronica → risposte automatiche

Tutte le mailbox sono configurate affinché eventuali comunicazioni email indirizzate al di fuori del dominio aziendale - destinatari diversi da ….@egas.sanita.fvg.it - riportino un messaggio in calce (disclaimer) nel quale viene dichiarata la natura non personale del messaggio nonché i vincoli in materia di riservatezza, con precisazione che le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente.

- È fatto divieto di utilizzare le caselle di posta elettronica su dominio @egas.sanita.fvg.it (come pure @dsc.fvg.it e @sanita.fvg.it) per motivi diversi da quelli strettamente legati all'attività lavorativa (ad esempio catene, messaggi personali, dibattiti, aste on line, concorsi, forum, mailing-list, ecc.).
- Non è consentito l'accesso a caselle di posta aziendali diverse da quella/e assegnate.
- Il personale assegnatario della casella di posta elettronica è responsabile del corretto utilizzo della stessa.
- Non è consentito l'utilizzo di caselle di posta elettronica personali, al di fuori di quella aziendale, per le comunicazioni istituzionali.
- È fatto divieto utilizzare le caselle di posta elettronica per motivi diversi da quelli legati all'attività lavorativa con l'eccezione dell'esercizio dei diritti normativamente tutelati per l'invio e la ricezione di informazioni di natura sindacale.
- È fatto obbligo ai singoli assegnatari delle caselle di posta uniformarsi alle modalità di firma delle e-mail di servizio (personali e non) in modo da garantire un contributo informativo omogeneo ed adeguato agli interlocutori dei dipendenti dell'Ente. Alla data di pubblicazione del presente documento, si richiama la "istruzione operativa per la firma delle e-mail di servizio".
- È obbligatorio porre la massima attenzione nell'aprire i file in allegato ai messaggi di posta elettronica, in particolare quando la provenienza risulti dubbia.
- Gli utenti sono tenuti a consultare regolarmente la posta elettronica aziendale.
- La dimensione massima di un file di posta è di 20Mb (allegati compresi), il gestore di posta blocca i messaggi in ingresso ed in uscita la cui dimensione ecceda tale limite. Nel

caso di invii che coinvolgono documenti pesanti, è consigliato l'utilizzo di formati compressi (*.zip, *.rar, *.tar, ..).

- La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti che alla lunga saturano lo spazio disponibile. Si ricorda a tal fine che sarà necessario eliminare anche i messaggi contenenti allegati di grandi dimensioni presenti nelle cartelle POSTA IN ARRIVO, POSTA INVIATA e CESTINO; si raccomanda inoltre di procedere all'eliminazione definitiva dei messaggi che vengono spostati nella cartella CESTINO utilizzando la voce SVUOTA evidenziando con il tasto destro del mouse la voce CESTINO.
- Le caselle di posta sono subordinate ad invii con un numero limitato e prestabilito di destinatari. Qualora sia necessario, per esigenze di servizio, modificare tale impostazione sarà necessario inoltrare apposita richiesta al Servizio Informativo (salvo casi particolari l'estensione del numero di destinatari viene concessa unicamente alle caselle di servizio non nominative).
- È previsto, come standard per ogni casella di posta, un dimensionamento massimo prestabilito; qualora fosse necessario un dimensionamento maggiore bisognerà farne richiesta al Servizio Informativo.
- La trasmissione informatica di documenti e dati con particolare requisiti di riservatezza ("categorie particolari" secondo il Regolamento UE 2016/679), deve essere effettuata secondo le modalità indicate nella sezione "ARCHIVI CON PARTICOLARI REQUISITI DI RISERVATEZZA".
- In caso di interruzione del rapporto di lavoro, siano essi cessazioni (mobilità in uscita, pensionamenti, dimissioni, ecc.) o sospensioni (aspettativa a vario titolo, congedi, utilizzo e comandi presso altri enti, ecc.), è onere del titolare della casella mail inserire per tempo idoneo messaggio automatico in relazione alla dismissione della cassetta postale.
- In caso di assoluta necessità è consentito al dirigente delegato di struttura accedere alla casella di posta elettronica dell'utente previa richiesta motivata al Servizio Informativo (POSTA ELETTRONICA ORDINARIA (PEO)).

Alla data di conclusione del rapporto di lavoro la struttura Politiche e Gestione Risorse Umane notificherà l'interruzione del rapporto di lavoro al Servizio Informativo indicandone la tipologia (cessazione o sospensione). Salvo diverse indicazioni, specifiche richieste e casi particolari che verranno opportunamente trattati, entro 3gg dal ricevimento della comunicazione, il Servizio Informativo procederà con la disabilitazione dell'utenza associata alla cassetta di posta impedendone l'accesso.

Per i soli di casi di cessazione del rapporto (mobilità in uscita, pensionamento, dimissioni o decesso), trascorsi ulteriori 60 giorni, periodo stimato pertinente e non eccedente a garantire l'operatività e la continuità di servizio, salvo diverse indicazioni degli assegnatari o dei responsabili, specifiche richieste e casi particolari che verranno opportunamente trattati, la cassetta di posta verrà definitivamente cancellata e non sarà possibile recuperare i dati (indirizzi, comunicazioni, ecc..) in essa contenuti.

In caso di sospensione del rapporto di lavoro, verrà valutata di concerto tra il Dirigente delegato e il soggetto interessato l'opportunità di procedere alla cancellazione o alla sospensione della casella e-mail personale.

L'utente in uscita ha facoltà di richiedere al Servizio Informativo la creazione di una copia (archivio .pst) della propria cassetta postale: è onere del richiedente la fornitura di un adeguato supporto di memorizzazione come pure la verifica di integrità dell'archivio stesso. È altresì onere dell'utente l'acquisto di appropriati strumenti software per la gestione dell'archivio rilasciato per il quale Egas non fornirà supporto alcuno. La richiesta di archiviazione, affinché

possa venir accolta, deve essere perfezionata prima del termine ultimo di cancellazione (60 giorni).
La cancellazione delle cassette mail di servizio non personali (ad es. concorso.infermieri@egas.sanita.fvg.it) avviene su specifica richiesta del dirigente delegato che ha in carico la gestione della casella stessa (o di suo superiore). In tal caso, contestualmente all'eliminazione, il Servizio Informativo procede d'ufficio creando un file archivio della cassetta da cancellare e consegnando il supporto rimovibile utilizzato (per esempio DVD, o file su share di rete) al dirigente delegato della casella. È onere del ricevente, istanziando eventualmente richiesta di supporto al Servizio Informativo, la verifica di integrità dell'archivio. Si ricorda che, trascorsi ulteriori 30gg, la cassetta online non risulterà ripristinabile.
L'utenza collegata alla mailbox non più utilizzata, non verrà eliminata (a differenza della casella di posta e dei contenuti della stessa), ma posizionata in un'apposita unità organizzativa in cui le utenze risultano disabilitate.

5.25 Posta elettronica certificata (PEC)

Nel caso di messaggi in cui sia necessario conservare la ricevuta di invio/ricezione risulta essenziale utilizzare la posta elettronica certificata (PEC), accessibile tramite gli strumenti messi a disposizione dal protocollo e dall'applicativo GIFRA.
La casella di posta elettronica istituzionale certificata (PEC) è lo strumento attraverso il quale l'azienda trasmette e riceve documenti informatici soggetti a registrazione di protocollo.
Di norma, non vengono concesse caselle di posta certificata personalizzate a meno di disposizioni normative diverse o specifiche richieste preventivamente autorizzate dal direttore generale.

- È obbligatorio, al fine di garantire la corretta conservazione a norma di legge, allegare esclusivamente la tipologia di file prescritti con nota Egas prot. 12695 "Conservazione Sostitutiva dell'Egas" dd. 11.05.2017, privilegiando, laddove possibile, l'utilizzo del formato PDF/A.

5.26 Spam e phishing

È fatto divieto di invio intensivo di posta elettronica indesiderata o invasiva (spam).
Qualora si ravvisassero casi di spam o di phishing (tipo di frode ideato allo scopo di rubare importanti dati personali dell'utente, come ad esempio numeri di carta di credito, password, dati relativi al proprio conto, ecc.) è necessario segnalare l'accaduto al gestore della piattaforma Exchange (Insiel S.p.A.).
La segnalazione deve avvenire allegando il messaggio incriminato in una nuova e-mail da inviare a: antispam@insiel.it, e specificando nell'oggetto la dicitura "Spam non fermato".

5.27 Social Network

Non è consentito l'utilizzo di alcun Social Network se non preventivamente autorizzato dalla Direzione Aziendale.
Il dipendente nell'utilizzo in forma privata, fuori dell'ambiente di lavoro, dei propri profili social è tenuto, anche in quanto pubblico dipendente, a non effettuare commenti denigratori o lesivi in genere della dignità di terzi e/o dell'Azienda. È altresì fatto assoluto divieto pubblicare qualsiasi contributo in forma di immagine o altro formato che possa essere lesivo della dignità, reputazione di terzi e/o dell'Azienda.
Quale conseguenza di utilizzo improprio dei propri profili social potranno essere attivati dall'Azienda meccanismi di rimborso del danno subito e potranno essere applicate sanzioni disciplinari.

L'Azienda, qualora approvasse l'utilizzo di Social all'interno dell'amministrazione, si riserva di attivare profili ufficiali aziendali strettamente correlati all'attività lavorativa.

5.28 Sistemi di videoconferenza

Non è consentito l'utilizzo di sistemi di videoconferenza/audioconferenza se non preventivamente autorizzati dal Servizio Informativo.
Alla data di pubblicazione del presente documento l'Egas sta completando l'avviamento di una piattaforma preposta alla gestione delle videoconferenze - affiancata da alcuni sistemi istituzionali - allo scopo semplificare la comunicazione tra i soggetti e minimizzando gli spostamenti necessari.

5.29 Richiesta di assistenza tecnica (help desk)

Alla data di pubblicazione del presente documento l'Assistenza alle postazioni è erogata da Insiel S.p.A.
In caso di mal funzionamento di uno o più sistemi informatici aziendali si procede contattando, negli orari di servizio, il telefono dell'Help-Desk al numero: 0432 557313.
L'Help-Desk prende in carico il problema segnalandolo ai Tecnici di competenza.
L'Utente dovrà fornire il nome macchina - o in alternativa l'indirizzo IP nei soli casi di indirizzamento statico - della postazione di lavoro sulla quale si è verificato il problema, il numero di telefono più vicino alla postazione, ed un nominativo di riferimento.
Dopo aver fornito questi dati dovrà farsi comunicare il numero della chiamata affinché, se l'intervento non viene eseguito in un tempo ragionevole, possa sollecitare una rapida soluzione del problema telefonando al numero stesso.

5.30 Uso personale di infrastruttura aziendale

Non sono previste modalità di utilizzo personale di mezzi informatici dell'Azienda con pagamento o fatturazione a carico dell'interessato.

6 Sistemi di controlli graduali e verifiche

L'Egas si riserva la facoltà di effettuare controlli mirati sul corretto utilizzo delle risorse informatiche. Qualora le misure indicate nella presente policy non fossero sufficienti a evitare comportamenti anomali, il personale del Servizio Informativo (o Insiel S.p.a per conto del Servizio Informativo) procederà con delle verifiche a livello di reparto, di ufficio, di gruppo di lavoro, in modo da individuare l'area da richiamare all'osservanza delle regole. Perdurando la situazione anomala, tali controlli, nelle forme e per le motivazioni di cui sopra, potranno essere effettuati su base individuale; all'esito degli stessi potrà essere avviato, nei confronti del dipendente interessato, regolare procedimento disciplinare nelle forme e nei modi di cui alla legge ed al CCNL applicato.
Tutti gli utenti sono tenuti a segnalare prontamente qualsiasi violazione alla presente Policy in forma non anonima. Viene comunque tutelato dall'Azienda il diritto alla privacy degli Utenti che comunicassero dette violazioni nei limiti previsti dalla normativa italiana.

6.1 Amministratori di sistema

Al fine di garantire le misure minime per la sicurezza delle tecnologie dell'informazione e della comunicazione (ICT) previste dalla vigente normativa sono previste delle forme di controllo affinché:

- gli amministratori di sistema utilizzino correttamente le utenze privilegiate, accedendo ai sistemi in uso con credenziali diverse da quelle non privilegiate;
- tutte le utenze, in particolare quelle amministrative, siano nominative e riconducibili ad una sola persona;
- tutte le utenze amministrative, siano debitamente e formalmente autorizzate.

La registrazione degli accessi effettuati dagli amministratori di sistema è svolta da parte del fornitore dello specifico servizio.

6.2 Rete Internet

Vista la delicatezza ed il carattere personale dei dati contenuti nei log verranno adottate tutte le cautele necessarie per evitare di pregiudicare il diritto alla riservatezza del lavoratore. L'Egas non utilizza sistemi hardware e software preordinati al controllo a distanza attraverso i quali sia possibile:

- effettuare controlli prolungati, costanti o indiscriminati;
- riprodurre e memorizzare sistematicamente le pagine Web visualizzate dal lavoratore;
- utilizzare strumenti di lettura e di registrazione dei caratteri inseriti tramite tastiera o analogo dispositivo;
- effettuare analisi occulta di computer portatili affidati in uso.

L'Egas riduce il rischio di usi impropri della "navigazione" in Internet, quali la visione di siti non pertinenti, l'upload o il download di file, l'uso di servizi di rete con finalità non autorizzate, adottando opportune misure che possono prevenire controlli successivi sul lavoratore.
In particole, sono adottate le seguenti misure:

- individuazione dei permessi di navigazione in Internet (accesso libero ad esclusione delle categorie di cui al punto successivo);
- l'utilizzo di sistemi di web filtering che inibiscono, preventivamente, l'accesso a siti dal contenuto chiaramente non attinente alle attività istituzionali, contrario al buon costume, potenzialmente pericoloso per la sicurezza e l'integrità dei dispositivi e dei servizi informatici aziendali e che prevengono determinate operazioni quali l'upload o l'accesso a determinati siti e/o il download di file o software aventi particolari caratteristiche;
- conservazione nel tempo dei dati (log) strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza;
- i soggetti autorizzati all'accesso delle informazioni di cui al punto precedente sono i gestori dell'infrastruttura proxy Regionale (Insiel S.p.A.) opportunamente incaricati;
- l'eventuale prolungamento dei tempi di conservazione sarà valutato come eccezionale e potrà avere luogo solo in relazione a:
    - esigenze tecniche o di sicurezza del tutto particolari;
    - indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
    - obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria;
- controlli saltuari o occasionali per ragioni legittime - verifiche sulla funzionalità e sicurezza del sistema - attraverso l'analisi puntuale dei log del Proxy Server da parte di personale autorizzato.

6.3 Posta elettronica ordinaria (PEO)

Tale regolamento è volto a sottolineare il carattere aziendale della posta elettronica quale strumento di lavoro del singolo dipendente, che, pertanto, non potrà essere utilizzato per finalità diverse. Il medesimo principio vale anche nel caso in cui il lavoratore utilizzi la casella di posta elettronica aziendale mediante il proprio dispositivo personale (smartphone, tablet, ecc..).
L'Egas adotta le seguenti soluzioni che consentano comunque lo svolgimento della regolare attività lavorativa:

- condivisione di indirizzi di posta elettronica tra più lavoratori;
- affiancamento dell'indirizzo condiviso con quello individuale; messa a disposizione di ciascun lavoratore di apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di assenze (ad es. per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" - elettroniche o telefoniche - di un altro soggetto o altre utili modalità di contatto della struttura e relative istruzioni sull'utilizzo (POSTA ELETTRONICA);
- in caso di eventuali assenze non programmate (ad es. per malattia), qualora il lavoratore non possa attivare la procedura sopra descritta, anche avvalendosi di servizi webmail, l'Egas dispone, sempre che sia necessario e mediante personale appositamente incaricato (es.: l'amministratore di sistema oppure l'incaricato alla gestione e manutenzione degli strumenti elettronici), l'attivazione delle procedure di cui al punto precedente, avvertendo gli interessati da parte del Dirigente delegato della struttura;
- conservazione nel tempo dei dati (log) dell'infrastruttura di posta Exchange, strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza;
- i soggetti autorizzati all'accesso delle informazioni di cui al punto precedente sono i gestori dell'infrastruttura di posta Regionale (Insiel S.p.A.) opportunamente incaricati;
- l'eventuale prolungamento dei tempi di conservazione sarà valutato come eccezionale e potrà avere luogo solo in relazione a:
    - esigenze tecniche o di sicurezza del tutto particolari;
    - indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
    - obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria;

6.4 Software

Periodicamente verranno effettuati controlli sulle macchine aziendali al fine di prevenire violazioni della legge a tutela del diritto d'autore sul software o rischi relativi alla sicurezza. Nel caso in cui vengano rinvenuti software non autorizzati installati su macchine aziendali, verranno immediatamente eliminati.
L'Egas procederà ad una verifica periodica del numero di licenze software presenti e, in caso di mancanza di alcune di esse, provvederà, se ritenuto necessario, alla loro integrazione, in caso contrario procederà alla rimozione del software non dotato di licenza.
Si invitano pertanto dipendenti e collaboratori a segnalare anomalie e mancanze in materia.

6.5 Dispositivi Personali

Nel caso di utilizzo di dispositivi personali per la gestione della casella di posta aziendale (ossia di proprietà dell'utente quali smartphone o tablet) attraverso il protocollo ActiveSync, è facoltà

dell'Azienda procedere alla formattazione del dispositivo da remoto nel caso venissero rilevate comprovate violazioni in termini di sicurezza (es. furto del dispositivo).
Lo stesso comportamento sarà adottato nel caso di assegnazione di analoghi dispositivi aziendali.

7 Sanzioni

È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con la presente Policy.
Il mancato rispetto o la violazione delle regole in essa contenute, qualora siano ravvisabili profili quantomeno colposi nella condotta osservata, è perseguibile nei confronti del personale dipendente mediante l'attivazione di procedimenti disciplinari previsti dalla vigente normativa e, rispettivamente, dai CCNL della Dirigenza sanitaria, professionale, tecnica ed amministrativa; della Dirigenza medica e veterinaria e del Comparto Sanità Personale non dirigente.

8 Tutela delle persone fisiche con riguardo al trattamento dei dati personali

La presente policy costituisce informativa agli interessati sul trattamento dei dati effettuati nel perseguimento del legittimo interesse di Egas alla corretta e completa gestione e controllo dell'utilizzo delle risorse informatiche nell'ambito del rapporto di lavoro e/o di collaborazione instaurato tenendo conto degli interessi e dei diritti e le libertà fondamentali degli interessati stessi.
Ai sensi dell'art. 13 del REG. UE 2016/679 - Regolamento Generale sulla Protezione dei Dati - relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e dell'art. 13 D. lgs. 196/2003 si rendono le seguenti ulteriori informazioni:

Titolare del trattamento
Ente per la Gestione Accentrata dei Servizi condivisi
Via Pozzuolo, 330
33100 Udine
Centralino: +39 0432 1438010
email: egas.protgen@certsanita.fvg.it

Dati di contatto del responsabile della protezione dei dati
RDP Egas - Via Pozzuolo n. 330 - 33100 Udine
telefono: 0432 554166
email: rpd@egas.sanita.fvg.it

I dati sono raccolti presso l'interessato e/o acquisiti da altri soggetti esterni ed elaborati sia in forma cartacea che elettronica e/o digitale. Il conferimento dei dati personali è necessario ai fini dello svolgimento delle attività descritte nel presente documento e l'eventuale rifiuto comporta l'impossibilità della prosecuzione del rapporto.

8.1 Categorie di destinatari dei dati personali

I dati sono resi accessibili a dipendenti e collaboratori autorizzati al loro trattamento nelle modalità descritte nel presente documento.
I dati possono essere resi accessibili a soggetti legati contrattualmente al Titolare (a titolo indicativo: fornitori di servizi, addetti all'assistenza hardware e software, istituti di credito,

studi professionali ecc.) che svolgono attività esternalizzate per conto del Titolare, anche eventualmente nella loro qualità di responsabili del trattamento.
I dati possono essere resi accessibili o comunicati ad Organismi di vigilanza, Autorità giudiziarie nonché a tutti gli altri soggetti ai quali la comunicazione sia obbligatoria per legge o per l'espletamento delle finalità per cui i dati sono raccolti.

8.2 Periodo di conservazione dei dati personali

Per quanto non diversamente previsto dal presente documento, si seguono i criteri di conservazione indicati dal "Prontuario di scarto" adottato dalla Direzione Generale per gli Archivi del Ministero per i beni e la attività culturali per quanto applicabili nonché le norme specifiche sulla conservazione e la vigilanza sugli archivi degli enti pubblici disposte dal Decreto Legislativo 22 gennaio 2004, n. 42, Codice dei beni culturali e del paesaggio, nonché la procedura per l'archiviazione dei documenti approvata con decreto n. 439/2010 dell'ex AOU "S. Maria della Misericordia" di Udine.

8.3 Diritti dell'interessato

L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali e di ottenere l'accesso ai dati personali e alle informazioni che lo riguardano.
L'interessato può esercitare in qualsiasi momento i seguenti diritti:
- chiedere al titolare del trattamento la rettifica dei dati inesatti o la limitazione del trattamento dei dati personali che lo riguardano nei casi previsti;
- chiedere la cancellazione dei dati personali che sono stati trattati illecitamente. Il diritto di cancellazione (all'oblio) non è riconosciuto in caso di adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
- opporsi al trattamento salvo l'esistenza di motivi legittimi prevalenti o cogenti per procedere al trattamento;
- proporre reclamo all'autorità Garante per la protezione dei dati personali.

9 Disposizioni finali, entrata in vigore e pubblicità

La Policy Egas per l'utilizzo delle risorse informatiche, proposta dal dirigente del Servizio Informativo, entra in vigore dalla data di esecutività del relativo Decreto di adozione.
Con l'entrata in vigore della presente Policy tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.
Per quanto non espressamente previsto nella presente policy sarà fatto riferimento alla normativa vigente in materia.
La presente Policy verrà debitamente e tempestivamente portata a conoscenza di tutti i dipendenti dell'Ente attraverso la pubblicazione sul sito internet istituzionale, verrà pubblicata su un'unità di rete accessibile a tutti gli utilizzatori e verrà inoltrata nota informativa a tutte le strutture aziendali.
È fatto obbligo di adeguare i propri comportamenti alle disposizioni previste nella presente policy ed a chiunque competa di osservarla.

10 Terminologie

Le seguenti terminologie si aggiungono alle definizioni di cui al regolamento UE 2016/679 alle quali si rinvia.

"autenticazione informatica": l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
"banca di dati": qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;
"comunicazione elettronica": qualsiasi comunicazione creata, inviata, inoltrata, trasmessa, archiviata, copiata, scaricata, mostrata, vista o stampata da uno o più sistemi o servizi di comunicazione elettronica;
"credenziali di autenticazione": le informazioni e/o i dispositivi, in possesso di una persona, solo da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;
"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;
"categorie particolari di dati personali ": i dati di cui all'art. 9 del UE 2016/679. Dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
"diffusione": il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
"dirigente delegato": i dirigenti dell'Ente, espressamente delegati dal titolare all'attuazione delle disposizioni in materia di trattamento dei dati;
"hardware": si indica la parte fisica di un computer, ovvero tutte quelle parti elettroniche, elettriche, meccaniche, magnetiche, ottiche che ne consentono il funzionamento (dette anche strumentario);
"help-desk": è un servizio che fornisce informazioni e assistenza ad utenti che hanno problemi nella gestione di un prodotto o di un servizio, cercando di risolvere il problema stesso direttamente o attraverso l'accesso da remoto da parte di personale addetto.
"incaricati": le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal dirigente delegato;
"interessato": la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
"laptop": Personal Computer portatile;
"misure minime di sicurezza ICT per le pubbliche amministrazioni": Le misure minime di sicurezza ICT emanate dall'AgID allo scopo di contrastare le minacce informatiche più frequenti della pubblica amministrazione italiana; consistono in controlli di natura tecnologica, organizzativa e procedurale, con tre livelli di attuazione
"parola chiave/password": componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;
"policy": documento che riporta obiettivi ed indirizzi generali, relativi alle principali funzioni ed attività assistenziali e gestionali;

"profilo di autorizzazione": insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;
"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
"risorse informatiche aziendali": qualsiasi combinazione di apparati tecnologici dell'Azienda e del SISSR, hardware o software, utilizzati per le comunicazioni elettroniche ed elaborazione dei dati;
"screensaver": salvaschermo ovvero applicazione per computer che provoca l'oscuramento dello schermo o la comparsa di un'animazione o di una serie di immagini in successione sullo stesso dopo un periodo programmato di inattività del mouse e della tastiera (non dell'elaboratore in sé), impostabile attraverso un timer;
"server di rete": elaboratore dedicato a cui competono funzioni di "computer centrale" in una rete locale di Personal Computer;
"servizi informatici aziendali": l'insieme delle apparecchiature e delle risorse (ivi compresi i programmi per elaboratore, i dispositivi elettromedicali e gli apparati per l'accesso alla rete di comunicazione elettronica Internet) che consentono all'Utente di accedere, visualizzare, modificare, e compiere ogni altra operazione su dati a qualunque titolo memorizzati nei dispositivi informatici aziendali, o da questi accessibili, nonché gli eventuali servizi ausiliari al loro funzionamento;
"sistema di autorizzazione": l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente;
"situazione d'emergenza": circostanza nella quale, il venir meno di un'azione, può provocare un serio pregiudizio a persone o cose, comportare il danneggiamento o la perdita di dati o impedire la verifica di una grave responsabilità dell'Azienda o degli Utenti della stessa;
"software": è l'informazione o le informazioni utilizzate da uno o più sistemi informatici e memorizzate su uno o più supporti informatici. Tali informazioni possono essere quindi rappresentate da uno o più programmi, oppure da uno o più dati, oppure da una combinazione delle due;
"spyware": sono programmi concepiti per raccogliere informazioni relative al PC e al suo possessore ed inviare il tutto via Internet al loro ideatore. La tipologia di informazioni sottratte può includere ma non essere limitata a: siti visitati, corredati di permanenza e file scaricati, siti Preferiti, contenuto della Cache e/o Cronologia del browser, configurazione hardware e software del PC, e molto altro. Il più delle volte lo scopo della sottrazione di informazioni è quello del marketing, ma potrebbe anche essere più dannoso.
"strumenti elettronici": gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
"titolare": 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;
"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;
"trojan horse": cavallo di troia, un programma apparentemente utile che nasconde le sue funzionalità; è dunque l'utente stesso che installando ed eseguendo un certo programma, inconsapevolmente, installa ed esegue anche il codice trojan nascosto. Spesso i trojan sono usati come veicolo alternativo ai worm e ai virus;
"username": il nome (identificativo) con il quale l'Utente viene riconosciuto da un computer, da un programma o da un server;
"utente": ciascuna persona che acceda alle Risorse informatiche aziendali;
"web": l'abbreviazione di World Wide Web, è un servizio di Internet che permette di navigare ed usufruire di un insieme vastissimo di contenuti collegati tra loro attraverso legami (link);
"webfiltering": un filtro web è un programma in grado di schermare una pagina Web in ingresso per determinare se alcuni o tutti vi accedono. Il filtro controlla l'origine o il contenuto di una pagina Web in base a una serie di regole fornite da società o persona che ha installato il filtro web ed inoltre, consente di bloccare le pagine di siti web che possono includere pubblicità discutibile, contenuti pornografici, spyware , virus ecc…, e altri contenuti discutibili;
"websecurity": consiste nel monitoraggio di tutte le informazioni sul traffico Internet;
"worm": sono programmi realizzati per riprodursi da un computer all'altro ma, a differenza dei virus, questa operazione avviene automaticamente. Per prima cosa i worm assumo il controllo delle funzioni del computer destinate al trasporto dei file o delle informazioni. Una volta presente nel sistema, il worm è in grado di viaggiare autonomamente.

11 Abbreviazioni

*BIOS: (*Basic Input-Output System) è un insieme di routine software, che fornisce una serie di funzioni di base per l'accesso all'hardware e alle periferiche integrate;
DCSISPS: Direzione centrale salute, integrazione sociosanitaria e politiche sociali;
PEO: Posta Elettronica Ordinaria. La PEO può essere "*ad personam*", associata ad una AOO, associata ad un ufficio, associata ad una specifica funzione/progetto o servizio.
AOO: Aree Organizzative Omogenee (AOO), identificano gli uffici di protocollo degli Enti che gestiscono i flussi documentali in entrata e in uscita dall'Ente.
PEC: Posta Elettronica Certificata;
INSIEL: Informatica per il Sistema degli Enti Locali S.p.A.: è una società in-house della Regione Friuli Venezia Giulia che si occupa della realizzazione degli sviluppi e della conduzione del SISSR;
IP: Internet Protocol è un'etichetta numerica che identifica univocamente un dispositivo collegato a una rete informatica (protocollo di comunicazione). Un indirizzo IP assolve due funzioni principali: identificare un dispositivo sulla rete e di conseguenza fornirne il percorso per la sua raggiungibilità da un altro terminale o dispositivo di rete. Può essere statico o dinamico;
LAN: Local Area Network: è un gruppo di computer connessi in un'area locale per comunicare tra loro e condividere risorse quali le stampanti, ecc…;
SISSR: Sistema Informativo Socio Sanitario Regionale coordinato della DCSISPS: è da intendersi come il complesso dell'infrastruttura telematica e delle procedure applicative condivise con tutte le aziende sanitarie della Regione Friuli Venezia Giulia;
VPN: Virtual Private Network: è una rete che permette a computer ubicati in sedi fisiche diverse di stabilire un collegamento

12 Riferimenti normativi e bibliografici

- UE 2016/679 “regolamento del parlamento europeo e del consiglio” relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati
- D.lgs 196/2003 “Codice in materia di protezione dei dati personali"
- D.lgs 101/2018 Disposizioni per l’adeguamento della normativa nazionale alle disposizioni del 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, nonche’ alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) (GU Serie Generale n.205 del 04-09-2018)
- Circolare 18 aprile 2017, n. 2/2017 - Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)»
- CAD - D. lgs 82/2005 “Codice dell’Amministrazione Digitale” e ss.mm.ii
- Linee Guida del Garante: “Lavoro: le linee guida del Garante per posta elettronica e Internet” - Del. n. 13 del 1° marzo 2007
- Provvedimento del Garante della Privacy - Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche - 2 luglio 2015
- Diritto D’autore - Legge 633/1941 “Protezione del diritto d’autore e di altri diritti concessi al suo esercizio” e ss.mm.ii (Legge 248/2000 “Nuove norme di tutela del diritto d'autore”)
- Legge 128/2004 “Conversione in legge, con modificazioni, del decreto-legge 22 marzo 2004, n. 72, recante interventi per contrastare la diffusione telematica abusiva di materiale audiovisivo, nonché a sostegno delle attività cinematografiche e dello spettacolo
- Codice civile artt. 2104 e 2105
- Statuto dei lavoratori - Legge n. 300/1970 “Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell’attività sindacale, nei luoghi di lavoro e norme sul collocamento”
- Provvedimento del Garante: “Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento - 25 giugno 2009” G.U. n. 149 del 30 giugno 2009.
- Provvedimento del Garante: “Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008” - G.U. n. 300 del 24 dicembre 2008.