Policy per il corretto utilizzo degli strumenti informatici

MATRICE DELLE REVISIONI					
Revisione	Data	Descrizione / tipo modifica	Redatta da	Verificata da	Approvata da
00	01/12/2020	Emissione	Nicola Bortolotti	Fabio Buffolini Elena Cussigh DPO	Giuseppe Tonutti
01					
02					
03					
04					
05					
06					

Sommario

1 Introduzione

Allo scopo di gestire e mitigare i rischi derivanti dall'utilizzo dei dispositivi informatici (è essenziale assicurare che le informazioni aziendali non siano compromesse), si rende necessario definire specifiche misure di sicurezza. Il presente regolamento disciplina 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 corsivo*- e fornendo fornisce informazioni in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse.

I requisiti da tenere in considerazione sono:

- censimento dei dispositivi
- protezione fisica
- restrizione sulle installazioni di software
- gestione delle versioni software e delle relative patch
- restrizioni per le connessioni a "information services"
- controllo degli accessi
- tecniche crittografiche
- protezione da malware
- disabilitazione, cancellazione e sblocco da remoto
- backup
- utilizzo di web app e web services

Qualora l'Azienda permetta l'utilizzo di dispositivi mobili personali, le misure di sicurezza dovranno altresì assicurare che l'uso distinto del dispositivo - per scopi lavorativi e personali – sia garantito tramite utilizzo di software preposto.

Qualora i dispositivi informatici contengano dati di particolare rilevanza per l'azienda da dover essere mantenuti riservati o dati personali si dovranno essere adottate misure di sicurezza adeguate.

2 Scopo

Il presente documento definisce le norme organizzative e comportamentali da rispettare nell'impiego dei dispositivi informatici da parte degli utilizzatori. In particolare, con la presente policy si intende promuovere, nel rispetto della normativa vigente, la diffusione di comportamenti corretti ed adeguati al fine di ridurre al minimo la probabilità di danni e perdite derivanti dall'uso improprio dei dispositivi.

I contenuti del documento, che si colloca all'interno delle politiche di Sicurezza, si applicano a tutti i dipendenti anche considerati come utenti finali o utilizzatori.

Questa policy di sicurezza riguarda tutti i dispositivi quali:

- smartphone, telefono cellulare;
- tablet;
- modem WiFi/MiFi, Aircard;
- postazioni di lavoro ("PdL" - PC, Laptop);

e ha lo scopo 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 della normativa in materia di protezione dei dati personali e, in particolare, dei principi di necessità, correttezza, pertinenza e non eccedenza;
- adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità dei sistemi informativi e dei 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.

3 Applicabilità

Questa Policy si applica a:

- a tutto il personale dipendente ed al personale autorizzato che utilizza le risorse informatiche dell'Azienda Regionale di Coordinamento per la Salute - di seguito "*l'Azienda*" o "*ARCS*" - 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 da ARCS 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.

Ogni soggetto sottoposto a questa politica deve comunque rispettare le leggi e le normative applicabili, anche se in conflitto con alcuni aspetti di questa politica; eventuali situazioni che dovessero portare ad un conflitto fra le leggi/normative e questa politica dovranno essere immediatamente segnalate alla struttura Tecnologie Informatiche (da ora T.I.).

4 Norme per l'utilizzo degli strumenti informatici

4.1 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 la struttura T.I. 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 dalla struttura T.I.; in assenza di autorizzazione è fatto divieto tassativo di connettere alla rete qualsiasi tipologia di apparato. Il collegamento dei dispositivi alla rete aziendale deve essere autorizzato dalla struttura T.I. secondo le modalità previste dalle procedure in essere (PROCEDURA PER IL COLLEGAMENTO IN RETE DI NUOVI DISPOSITIVI). *La procedura per il collegamento in rete di un nuovo dispositivo prevede il cambio delle credenziali dell'amministratore predefinito del dispositivo.*

La struttura T.I. 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 responsabile della struttura coinvolta e del responsabile della struttura T.I.

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

- devono essere custoditi con cura e 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);
- non devono essere ceduti, neppure temporaneamente (a meno di dispositivi assegnati a livello di struttura), a terzi, né a titolo gratuito né a titolo oneroso;
- 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.
- è fatto obbligo all'utente utilizzatore di rimuovere eventuali file elaborati ed utilizzati, prima della riconsegna - particolare attenzione è richiesta nel caso di un utilizzo temporaneo del PC portatile assegnato.

- 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;
- Nel caso in cui si riscontrasse una violazione delle regole di conservazione degli strumenti assegnati, l'azienda potrà avviare procedimenti disciplinari e chiedere il rimborso dell'eventuale danno subito.

4.2 Utilizzo del PC

Il Personal Computer (PC) è uno strumento di lavoro affidato al Dipendente, di cui lo stesso è responsabile sia per la parte Hardware che Software. Il PC deve essere utilizzato per i soli ambiti inerenti all'attività lavorativa; eventuali informazioni salvate -anche temporaneamente- sulla postazione di lavoro, devono pertanto riguardare esclusivamente la propria attività lavorativa. Ogni utilizzo del PC non afferente alla propria attività lavorativa può contribuire ad innescare disservizi, costi di assistenza e manutenzione e, soprattutto, minacce alla sicurezza dell'intera rete aziendale e/o delle reti telematiche e dei sistemi informatici di terzi esponendo l'organizzazione e gli stakeholder aziendali a crimini informatici.

Tutti i dipendenti di ARCS sono a conoscenza che i dati conservati nel proprio Personal Computer, compresi i messaggi di posta elettronica in entrata e in uscita, possono essere visionati dai Responsabili della struttura in caso di necessità dovute a titolo esemplificativo e non esaustivo, a malfunzionamenti del sistema, esigenze lavorative, assenza dell'Incaricato, ecc... I Responsabili di struttura, pertanto, per l'espletamento delle loro funzioni, hanno la facoltà in qualunque momento di accedere ai dati trattati dai propri collaboratori, ivi compresi gli archivi di posta elettronica in entrata ed uscita, chiedendo formalmente accesso alla struttura T.I.

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); *sulle postazioni di lavoro (fisse e laptop) di ARCS è stata implementata una policy che prevede il blocco automatico della postazione dopo alcuni minuti di inattività*.

Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio: lasciare un elaboratore per lungo tempo incustodito, 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 ogni caso deve essere attivato lo screensaver con richiesta di password per lo sblocco.

4.3 Credenziali di accesso ai dispositivi e alla rete

L'accesso all'elaboratore è protetto da codice identificativo e password (credenziali), che devono essere custoditi con la massima diligenza e non divulgate.

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 della struttura T.I. 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 Gestione Risorse Umane ne dà tempestiva comunicazione alla struttura T.I. 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 password 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 afferente alla struttura T.I. - previo appuntamento e munito di documento di identità in corso di validità.

Per maggiori informazioni e approfondimenti si prega di fare riferimento alla sezione UTILIZZO DELLE CREDENZIALI e alla procedura aziendale preposta GESTIONE DELLE CREDENZIALI E DEI PROFILI DI ACCESSO.

4.4 Credenziali di accesso ai servizi e agli applicativi

I Responsabili di struttura o loro 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 responsabile (o suo delegato) della struttura/ufficio/area con il quale il collaboratore si coordina nell'espletamento del proprio incarico.

Ogni struttura 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 responsabile di struttura (o suo delegato) dell'utente in uscita dovrà compilare la modulistica preposta ed inviarla alla struttura T.I. per l'immediata sospensione delle credenziali di accesso agli applicativi gestionali.

Per maggiori informazioni e approfondimenti si prega di fare riferimento alla sezione UTILIZZO DELLE CREDENZIALI e alla procedura aziendale preposta GESTIONE DELLE CREDENZIALI E DEI PROFILI DI ACCESSO.

4.5 Caratteristiche delle credenziali di accesso

Gli utenti 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 dalle ultime 10 password precedentemente utilizzate;
- 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.

Qualora le limitazioni tecniche del sistema non permettano la configurazione dello stesso al fine di limitare selettivamente l'utilizzo di password "robuste", sarà onere dell'utilizzatore l'impostazione di password secondo le specifiche in precedenza elencate.

4.1 Utilizzo delle credenziali

L'utente è tenuto a rispettare i criteri descritti nella sezione *Caratteristiche delle credenziali di accesso* 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 dell'Azienda che di

terzi, 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 (quali post-it, quaderni, ecc…) 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, o sia noto a terzi, dandone comunicazione alla struttura T.I.

Nel caso l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia all'Amministratore di sistema ed alla struttura T.I.

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.

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.

4.1 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 "Amministratori di Sistema" (decreto ARCS n.189 del 26.08.2020).

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 "*Caratteristiche delle credenziali di accesso*", devono essere soggette a maggiori requisiti di complessità, in particolare:

- deve essere di lunghezza non inferiore ad 16 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 dalle ultime 10 password precedentemente utilizzate;

- 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.

Qualora le limitazioni tecniche del sistema non permettano la configurazione dello stesso al fine di limitare selettivamente l'utilizzo di password "robuste", sarà onere dell'utilizzatore l'impostazione di password secondo le specifiche in precedenza elencate.

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 dalla sola struttura T.I. 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).

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 della struttura T.I.).

4.2 Utilizzo dei supporti rimovibili

Tutti i file di provenienza incerta o esterna -ancorché attinenti all'attività lavorativa- devono essere sottoposti a controllo antivirus prima di essere aperti e/o utilizzati.

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.

Non è permesso scaricare o copiare file contenuti in supporti removibili esterni (USB, hard disk drive, "chiavette USB", ecc..) se non attinenti alla propria attività lavorativa.

In particolare, nel caso di assegnazione di dispositivo di memoria esterno (USB), l'uso è autorizzato -previa compilazione dell'apposito modulo di consegna- esclusivamente se:

- il device è stato preventivamente cifrato con tecnologia Bitlocker (tassativamente a cura della struttura T.I.);
- l'utente si obbliga a non scaricare (copiare/spostare) i file contenuti nella memoria USB, su dispositivi (PdL, laptop, ecc …) diversi da quelli aziendali ARCS;
- l'utente si impegna a non diffondere nè comunicare a terzi per alcuna ragione la chiave di cifratura, a conservarla in luogo protetto - separato dal dispositivo stesso- e a non modificare la stessa senza previa ed esplicita autorizzazione della struttura T.I.

Nel caso in cui dati, informazioni, immagini e/o notizie aziendali e/o dati riservati devono essere salvate su supporti removibili, è obbligatorio conservare, custodire e controllare tali supporti affinché nessun soggetto terzo non autorizzato ne prenda visione o possesso. L'utente assegnatario è l'unico responsabile della custodia dei supporti e dei dati in essi contenuti.

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.

I supporti rimovibili contenenti dati 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 o consegnati alla struttura T.I. per la loro corretta gestione/dismissione.

4.3 Unità di rete, memorizzazione file e backup

Il disco fisso locale del proprio PC deve essere utilizzato per la sola memorizzazione di file di interesse aziendale. La memorizzazione deve essere limitata a poche ore lavorative dal momento che questi

dischi non sono sottoposti a backup. Tutti i file di rilevanza aziendale devono essere salvati sulle aree comuni o sulle aree personale delle share di rete (server preposto). È assolutamente da evitare la conservazione in rete di file obsoleti e/o inutili e/o ridondanti e per questo si invita il dipendente ad un attento ed ordinato utilizzo dello spazio di rete.

Qualsiasi file estraneo all'attività lavorativa e/o non espressamente autorizzato, non può, nemmeno in via transitoria, essere salvato sul PC in uso del dipendente e tanto meno essere salvato sulla rete aziendale.

La competenza e la gestione delle aree di interesse comune è demandata ai responsabili di funzione di ciascuna area che provvederà ad indicare ai propri collaboratori i criteri sulle modalità di salvataggio e protocollo dei documenti.

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. Per il ripristino dei dati accidentalmente persi o modificati sulle cartelle di rete è fatto obbligo di avvisare tempestivamente la struttura T.I.

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.

ARCS si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericoloso per la sicurezza aziendale ovvero acquisiti o installati in violazione della presente policy; pertanto, gli amministratori di sistema preventivamente abilitati, senza necessità di esplicita autorizzazione, hanno facoltà di procedere alla verifica ed eventuale rimozione di qualsiasi file memorizzato nelle cartelle di rete (o in locale sulla PdL) qualora ritenuto pericoloso per la sicurezza o non attinente all'attività lavorativa.

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 della struttura T.I., 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 responsabile di struttura (o suo 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 la struttura T.I.
Ove possibile, la struttura T.I. metterà a disposizione degli utenti che ne facessero richiesta, per il tramite del proprio responsabile di struttura (o suo 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 Gestione Risorse Umane notificherà l'interruzione del rapporto alla struttura T.I. 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 personale della struttura T.I. procederà *alla variazione dei permessi della cartella di rete concessa in maniera esclusiva (qualora richiesta) affinché sia consentito al responsabile di struttura, 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 personale della struttura T.I. procederà alla cancellazione definitiva della cartella di rete assegnata in modalità esclusiva e non sarà possibile recuperare i dati in essa contenuti*.

4.4 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). Per maggiori informazioni si rimanda alla procedura PROTEZIONE CRITTOGRAFICA E TRASMISSIONE DI DOCUMENTI CON PARTICOLARI REQUISITI DI RISERVATEZZA.

4.5 Utilizzo carte operatore (firma digitale)

I Responsabili di struttura 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, la cui durata massima del certificato di firma è pari a 12 mesi e la durata del certificato di autenticazione 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 assegnatario della carta contattare la struttura T.I. 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 alla struttura T.I. 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 adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri

4.6 Utilizzo interno ed esterno della posta elettronica ordinaria (PEO)

L'indirizzo e-mail assegnato da ARCS ai dipendenti è uno *strumento di lavoro di proprietà aziendale concesso in uso al lavoratore per un più proficuo svolgimento della prestazione*. La Posta Elettronica Ordinaria - PEO - può essere rilasciata "ad personam", associata ad un ufficio o ad una specifica funzione/progetto/servizio. Le persone assegnatarie delle caselle sono responsabili del corretto utilizzo delle stesse.

La casella assegnata "ad personam" ha il seguente formato <nome>.<cognome>@arcs.sanita.fvg.it (in caso di omonimia verrà aggiunto un progressivo numerico, quindi <nome>.<cognome>2@arcs.sanita.fvg.it, <nome>.<cognome>3@arcs.sanita.fvg.it, ecc...). Tale

indirizzo va utilizzato in via esclusiva per tutta la corrispondenza elettronica in entrata ed in uscita. È espressamente vietato utilizzare caselle di posta diverse da quella assegnata reperibili in Internet, quali webmail fornite, ad esempio, da Yahoo, Libero, Hotmail, etc…

Possono essere assegnate, qualora si rendesse necessario per esigenze organizzative del lavoro e dietro specifica richiesta del responsabile di struttura (o suo delegato), delle caselle di posta del tipo: tecnologie.informatiche@arcs.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 responsabile (o suo delegato) della struttura interessata verificare l'esistenza di tale casella e, in caso negativo, farne richiesta alla struttura T.I. 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.

Anche l'accesso alla mail di servizio non personale, se autorizzato, avviene con le credenziali personali.

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.

Il dipendente è responsabile del contenuto dei messaggi inviati: al fine di garantire la sicurezza dei sistemi informativi aziendali *è vietato utilizzare le caselle di posta assegnate per l'invio di messaggi personali o di contenuto extra lavorativo* (con l'eccezione dell'esercizio dei diritti normativamente tutelati per l'invio e la ricezione di informazioni di natura sindacale).

È proibita ai dipendenti, salvo consenso espresso del responsabile per comprovate esigenze lavorative, la sottoscrizione a mailing list, newsletter ed altri contatti. È vietato diffondere "messaggi broadcast" (messaggi a diffusione capillare e moltiplicata) che moltiplicano più volte i messaggi su tutte le caselle di posta.

Non è consentito l'utilizzo di caselle di posta elettronica personali, al di fuori di quella aziendale, per le comunicazioni istituzionali. Non è altresì permesso l'utilizzo di caselle di posta aziendali diverse da quella/e assegnate.

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'Azienda. I messaggi in uscita dovranno riportare in calce gli estremi identificativi e il ruolo aziendale dell'Incaricato, nonché il disclaimer predisposto. Tutte le mailbox sono configurate affinché eventuali comunicazioni email indirizzate al di fuori del dominio aziendale riportino un messaggio in calce 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. Per maggiori informazioni fare

riferimento al Decreto del direttore generale ARCS n. 93 del 17/04/2020 "ADOZIONE DEL "MANUALE DI STILE" DEL COORDINATO AZIENDALE PER LA DOCUMENTAZIONE E PER LA CARTELLONISTICA INTERNA".

I dipendenti sono tenuti a verificare frequentemente i messaggi pervenuti all'indirizzo loro assegnato, e, per quanto possibile, a dare loro l'esito appropriato immediatamente (riscontrandone la ricezione, rispondendovi direttamente, inoltrandoli ad altri utenti del dominio @arcs.sanita.fvg.it e scadenzando le incombenze opportune, …)

Gli allegati ai messaggi in entrata in formato non intrinsecamente sicuro vanno sempre verificati con il sistema Antimalware pre-installato prima di qualsiasi altra iniziativa quando non ne sia personalmente noto il mittente.

Nel caso di messaggi inviati ad un numero consistente di destinatari va evitato che compaia l'elenco degli indirizzi dei destinatari, e ciò mediante utilizzo della funzione "blind courtesy copy" (ccn).

Nel caso in cui si debba inviare un documento all'esterno dell'Azienda è preferibile utilizzare un formato protetto da scrittura, o in genere non modificabile (ad esempio il formato Acrobat *.pdf).

L'inoltro a terzi di messaggi ricevuti deve essere riconoscibile come tale nell'oggetto e deve essere giustificato da ragioni obbiettive.

Gli allegati vanno menzionati nel corpo del messaggio con indicazione del loro contenuto, se possibile trasmessi in formato universale e sicuro (PDF/A). Nel caso sia assolutamente necessario inoltrare all'esterno allegati ricevuti dall'esterno in formati non intrinsecamente sicuri, va altresì espressamente declinata ogni responsabilità al riguardo nel corpo del messaggio.

Tutti i messaggi e-mail da e per l'esterno sono equiparati alla corrispondenza cartacea inviata e ricevuta per ragioni connesse con l'attività svolta dall'azienda. Tutti i messaggi e-mail da e per l'esterno sono, pertanto, di esclusiva disponibilità dell'Azienda, che potrà accedervi in qualsiasi momento, considerati i fini per cui tale utilizzo è ammesso ai sensi della presente policy. All'azienda compete altresì ogni decisione circa l'impiego dei messaggi e-mail (da e per l'esterno) e sull'esercizio dei diritti agli stessi connessi. Non sono ammessi contenuti ed utilizzi diversi da quelli richiesti dalle finalità lavorative ed organizzative proprie dell'Azienda per il cui raggiungimento l'Azienda acconsente all'impiego di tale strumento.

È fatto divieto di inviare messaggi e-mail (interni ed esterni) che siano illegali, diffamatori, discriminatori o altrimenti contrari a norme di legge e che possano essere in qualunque modo fonte di responsabilità dell'Azienda e/o del singolo utente.

È vietato inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinioni e appartenenza sindacale e/o policy. Nel caso di invio di messaggi che siano reputati lesivi dell'immagine e della moralità dell'Azienda, l'Azienda provvederà ad effettuare gli opportuni accertamenti e ad intraprendere le iniziative legali che si renderanno necessarie.

È fatto divieto di manomettere, modificare o alterare in qualsiasi modo i messaggi e-mail, sia ricevuti che inviati, siano essi interni o da e per l'esterno.

È assolutamente vietata la comunicazione a terzi di informazioni riservate (confidenziali), segrete, o che siano comunque di rilievo per ARCS e per la sua attività, nonché di qualsiasi informazione di natura riservata appresa e/o delle quali il dipendente sia venuto a conoscenza durante lo svolgimento della propria attività, in violazione dell'obbligo di fedeltà e correttezza a carico dei dipendenti (a titolo esemplificativo e non esaustivo piani strategici, informazioni inerenti a due diligence, dati personali inerenti a interessati ecc.). È vietato divulgare notizie, dati e qualsiasi altra informazione appresa in occasione della ricezione o invio di posta elettronica, in quanto coperte dal segreto professionale cui sono tenuti i dipendenti.

Nel caso di mittenti sconosciuti o messaggi insoliti, prima di aprire il file, è necessario ispezionarlo con una verifica approfondita -chiedendo eventualmente supporto alla struttura T.I.- e, se necessario, cancellare i messaggi senza aprirli per non correre il rischio di essere infettati da malware, o in genere, virus ed esporre l'organizzazione a crimini informatici.

Nel caso di messaggi provenienti da mittenti conosciuti ma che contengono allegati sospetti (file con estensione .exe .scr .pif .bat .cmd .msi o in genere non noti all'utente), è vietato aprire gli alleati e/o salvare ed eseguire i file.

In caso di assenza, il dipendente ha a disposizione apposite funzioni di sistema che consentono di inviare automaticamente messaggi di risposta (fuori sede).

In caso di assoluta necessità è consentito al responsabile di struttura accedere alla casella di posta elettronica del proprio collaboratore previa motivata richiesta alla Direzione aziendale (e alla struttura T.I. per la parte operativa di delega all'accesso).

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 procedura preposta PROTEZIONE CRITTOGRAFICA E TRASMISSIONE DI DOCUMENTI CON PARTICOLARI REQUISITI DI RISERVATEZZA.

Alla data di conclusione del rapporto di lavoro la struttura Gestione Risorse Umane notificherà l'interruzione del rapporto di lavoro alla struttura T.I. indicandone la tipologia (cessazione o sospensione). Salvo diverse indicazioni, specifiche richieste e casi particolari che verranno opportunamente trattati, entro 3gg dal ricevimento della comunicazione, la struttura T.I. 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 loro responsabili, specifiche richieste e casi particolari che verranno opportunamente trattati, la cassetta di posta verrà

definitivamente cancellata e non sarà possibile recuperarne i dati (indirizzi, comunicazioni, ecc..) in essa contenuti.

In caso di sospensione del rapporto di lavoro, verrà valutata di concerto tra il responsabile di struttura 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 alla struttura T.I. 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 ARCS 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.2015@arcs.sanita.fvg.it) avviene su specifica richiesta del responsabile di struttura che ha in carico la gestione della casella stessa (o di suo superiore). In tal caso, contestualmente all'eliminazione, la struttura T.I. 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 responsabile di struttura della casella. È onere del ricevente, istanziando eventualmente richiesta di supporto alla struttura T.I., 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.

ARCS si riserva la facoltà, nei limiti stabiliti e consentiti dalla normativa vigente, di verificare che quanto sopra esposto sia scrupolosamente seguito dai soggetti interessati. Le violazioni delle disposizioni concernenti l'uso della posta elettronica contenute nella presente policy può comportare l'applicazione delle sanzioni disciplinari previste dal CCNL in vigore.

4.7 Utilizzo interno ed esterno della 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.

Nell'utilizzo della PEC risulta obbligatorio, al fine di garantire la corretta conservazione a norma di legge, allegare esclusivamente la tipologia di file prescritti con nota ARCS prot. 12695 CONSERVAZIONE SOSTITUTIVA DELL'ARCS dd. 11.05.2017, privilegiando, laddove possibile, l'utilizzo del formato PDF/A.

4.8 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".

4.9 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 procedimenti disciplinari a carico del responsabile e richieste di risarcimento dei danni eventualmente subiti da ARCS.

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

4.10 Network ARCS

4.10.1 Utilizzo della rete fisica locale (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*.

La rete aziendale interna non può esser utilizzata per scopi diversi da quelli ai quali è destinata. Il dipendente che si renda conto che nella rete interna circolano dati, notizie ed informazioni non

pertinenti l'attività lavorativa o che possono essere riconducibili ad illecito è tenuto ad informare immediatamente il proprio responsabile e la struttura T.I.

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 alla struttura T.I. e ricevere autorizzazione dalle Direzioni competenti. Analogamente non è ammesso, se non per esigenze estemporanee e previa autorizzazione della struttura T.I., l'utilizzo non autorizzato di dispositivi per lo sdoppiamento di punti rete (mini Hub/switch).
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 della struttura T.I. 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, DHCP, NTP, 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 afferente alla struttura T.I. 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 della struttura T.I. 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.

4.10.2 Utilizzo della rete Wireless (WLAN)

Ad integrazione della rete LAN descritta nella precedente sezione UTILIZZO DELLA RETE FISICA LOCALE (LAN), alcune aree dell'ARCS sono servite da reti non cablate -Wireless LAN- per consentire la trasmissione dei dati attraverso canali senza fili. Utilizzando specifici apparati Access Point vengono distribuiti due SSID: "*arcs-ospiti*" ed "*arcs-enterprise*".

La WiFi-LAN "*arcs-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. La

tecnologia è configurata e governata da Insiel S.p.A., ed ARCS dispone il rilascio delle abilitazioni per il tramite della struttura T.I.

È fatto divieto assoluto di connettersi a tale infrastruttura utilizzando sistemi diversi dai dispositivi aziendali quali portatili e tablet preventivamente configurati dalla struttura T.I. (per esempio, è vietata la connessione di cellulari, oppure laptop e tablet personali).

4.10.3 Internet

Il PC abilitato alla navigazione in Internet costituisce uno strumento necessario allo svolgimento della propria attività lavorativa. È pertanto vietato accedere a siti il cui contenuto non è riconducibile all'attività lavorativa. *L'abilitazione alla navigazione è assegnata a livello di utenza* e deve essere autorizzata dal responsabile di struttura (o suo delegato) che invia opportuna richiesta alla struttura T.I.

È attivo un sistema di protezione della navigazione Internet che prevede il filtraggio automatico del traffico per categorie di contenuti ed è inoltre presente la funzionalità di gestione di specifiche blacklist di url.

È vietata la connessione alla rete Internet mediante l'autonoma installazione di modem, router o altri apparecchi di connettività.

Non è consentito scaricare o copiare (download/upload di) file o software di ogni genere da siti internet accedendo abusivamente ad un sistema informatico o telematico protetto da misure di sicurezza. Allo stesso modo non è consentita la permanenza in un sistema informatico o telematico, servizio applicativo in genere contro la volontà espressa o tacita dell'Azienda. ARCS si cautela nei confronti di tali attività bloccando l'accesso a siti Internet non pertinenti l'attività lavorativa e comunque tracciando tutte le attività di navigazione effettuate all'interno dell'azienda stessa.

Ogni file (o software) eventualmente scaricato da Internet avviene sotto la responsabilità esclusiva di ciascun dipendente e deve essere necessariamente preceduto da una analisi volta a verificare l'eventuale presenza di virus; ciò a tutela dell'integrità del patrimonio aziendale. Qualora il singolo utilizzatore dipendente non sia in grado di procedere autonomamente e correttamente al predetto controllo, dovrà contattare la struttura T.I., prima di procedere a qualsiasi operazione che comporti il prelevamento di file da siti Internet.

Non è consentito l'utilizzo dei servizi di messaggistica istantanea -esclusi quelli espressamente autorizzati dall'azienda- programmi di condivisione file (file sharing) e di programmi P2P.

È rigorosamente vietata la registrazione e partecipazione a forum non professionali, l'utilizzo di chat-line, di social network, di bacheche elettroniche (esclusi quelli espressamente autorizzati dall'azienda) le registrazioni in guest books anche utilizzando pseudonimi.

Non è consentita alcuna attività legata ad operazioni di hackeraggio e pirateria informatica in generale.

È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo i casi direttamente autorizzati dai Responsabili e con il rispetto delle normali procedure d'acquisto.

4.11 Hardware e configurazioni di sistema

L'hardware potrà essere acquistato solo previa autorizzazione della struttura T.I. 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 responsabile della struttura/ufficio/area, ed indirizzate al responsabile della struttura T.I. ed al responsabile del Provveditorato Centralizzato.

Non è consentito l'utilizzo di hardware di tipo personale salvo specifica autorizzazione della struttura T.I.

Non è consentita l'installazione autonoma di alcun dispositivo di memorizzazione, comunicazione o altro (per quanto attinente ai dispositivi esterni consultare la sezione UTILIZZO DEI SUPPORTI RIMOVIBILI.

Non è consentito all'utente modificare le caratteristiche hardware e software del PC (fisso e mobile) in dotazione, 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 della struttura T.I.
Non è consentito all'utente procedere all'installazione di dispositivi di memorizzazione, comunicazione o altro (es. masterizzatori, modem, etc.) in assenza di preventiva autorizzazione da parte della struttura T.I.
Non è consentito lo spostamento del PC e delle relative periferiche senza preventiva esplicita autorizzazione da parte della struttura T.I.

Per ciascuna tipologia di hardware in 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, sono clonate utilizzando master disk - aderenti alle misure minime di sicurezza ICT per le pubbliche amministrazioni- appositamente realizzati per le specifiche necessità dell'ARCS. *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).*

Alla data di pubblicazione del presente documento, in Azienda è attiva una configurazione basata su Dominio Microsoft Windows e Active Directory. Sono stati installati due Domain Controller distribuiti sul territorio.

Tutte le macchine vengono connesse al dominio attraverso un'operazione di "join" e legate al distributore antivirus dedicato alle postazioni di lavoro dell'ARCS; i Personal Computer aziendali (PdL fisse) devono pertanto 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 dalla struttura T.I.

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.
La struttura T.I. si riserva la facoltà di bloccare in qualsiasi momento le interfacce USB delle stazioni di lavoro per impedire l'utilizzo di supporti di massa.

Per peculiari necessità operative, alcune postazioni, strettamente destinate alla gestione delle emergenze, sono fornite e gestite da INSIEL S.p.A. 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.

4.12 Installazione software

L'installazione di software deve avvenire esclusivamente ad opera di soggetti provvisti di specifiche abilitazioni preventivamente autorizzati dalla struttura T.I.

I software e gli applicativi installati sono parte del patrimonio aziendale e come tali devono essere utilizzati nel rispetto della presente policy e di eventuali indicazioni ricevute dalla struttura T.I.

Al fine di tutelare il sistema informatico -sussistendo il grave pericolo di introdurre codice malevolo e/o di alterare la funzionalità delle applicazioni software esistenti- *è fatto divieto a chiunque utilizzi computer aziendali di scaricare dalla rete Internet (installare e/o eseguire) qualsiasi tipo di software non autorizzato*.

Non è consentito l'utilizzo di software che consenta l'accesso alla postazione di lavoro - controllo remoto - o ai dati istituzionali al di fuori della rete aziendale (condivisione dati online), ad esclusione degli eventuali applicativi preventivamente forniti ed autorizzati dalla struttura T.I.

Al fine di tutelare l'integrità e la veridicità dei documenti informatici, è vietata la installazione e l'utilizzo di software (e hardware) atti ad intercettare, falsificare, alterare, impedire e interrompere comunicazioni (e/o il contenuto documenti informatici); è altresì vietata l'installazione di software che potrebbero rivelarsi lesivi del sistema informatico aziendale.

Non è permesso l'utilizzo di programmi diversi da quelli ufficialmente installati dalla struttura T.I. -o dall'Insiel S.p.A. per conto di ARCS- 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, comprese 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.

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 della struttura T.I. di intervenire per effettuare l'installazione.

L'installazione volontaria sul personal computer in dotazione di componenti software in grado di danneggiare, deteriorare o rendere, in tutto o in parte, inservibile il sistema informatico o le informazioni in esso contenute, può costituire, tenuto conto della gravità del comportamento, condotta sanzionata penalmente ai sensi dell'art. 635-bis Cod. Pen.

Sono in uso particolari software 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.

Gli aggiornamenti del sistema operativo sono necessari, oltre che per 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*.

È tassativamente vietato all'utente ogni sorta di aggiornamento manuale del software installato se non espressamente autorizzato dalla struttura T.I. Gli aggiornamenti del software e dei driver necessari al buon funzionamento della postazione di lavoro saranno effettuati direttamente dai tecnici della struttura T.I. (o da Insiel S.p.A. per conto dell'ARCS) 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.

4.13 Gestione delle vulnerabilità tecniche

Al fine di migliorare la sicurezza generale di tutta l'infrastruttura e rispondere ai requisiti imposti dall'AgID, ARCS impiega un servizio di verifica delle vulnerabilità tecniche; per maggiori informazioni si rimanda alla PROCEDURA PER LA GESTIONE DELLE VULNERABILITÀ.

4.14 Antimalware

L'ARCS 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. Sulle 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. Non è ammesso l'utilizzo di sistemi antivirus diversi, se non espressamente autorizzato dalla struttura T.I. 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; nell'eventualità si ravvisasse la mancanza di tale software l'utente dovrà darne immediata segnalazione alla struttura T.I. per procedere alla sua installazione.

È vietato disabilitare il sistema antivirus o bloccarne l'automatico aggiornamento sul PC concesso in uso al dipendente: ogni dipendente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico da parte di virus o ogni altro software aggressivo.

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 preposto secondo le vigenti disposizioni.

4.15 Utilizzo degli apparecchi telefonici

L'apparecchio telefonico di rete fissa e mobile costituisce uno strumento necessario allo svolgimento dell'attività lavorativa. È consentito l'uso, salvi casi eccezionali di obiettiva necessità o preventivamente autorizzati, per fini personali utilizzando il servizio di *Dual Billing*, così come descritto nelle procedure aziendali.

I dati telefonici relativi alla durata delle chiamate, al numero destinatario delle stesse e all'identificazione del numero interno chiamante, possono essere rilevati dalla struttura T.I. ai fini dell'imputazione dei centri di costo e sono conservati per due anni.

ARCS non procede ad alcuna rilevazione del contenuto delle conversazioni telefoniche, salvo nei servizi per i quali ne è stata concessa motivata e formale autorizzazione.

In caso di furto o smarrimento del telefono, deve essere immediatamente informata la direzione e la struttura T.I. in modo da bloccare remotamente il telefono. In caso di furto deve essere fornita in copia all'azienda la denuncia presentata agli organi competenti. In caso si ravvedesse una negligenza da parte dell'utente, ARCS ha la facoltà di trattenere a titolo di risarcimento, mediante ritenuta in busta paga, l'importo che necessario alla riacquisizione del bene. Per una corretta gestione della sicurezza, il telefono dovrà sempre essere configurato affinché, per sbloccare l'apparecchio dalla modalità stand-by, venga utilizzato il lettore di impronta digitale o, in alternativa, il PIN. È altresì obbligatorio l'utilizzo del PIN di sicurezza per il blocco/sblocco della SIM.

Il telefono cellulare deve risultare attivo e raggiungibile, se le condizioni tecniche lo consentono, durante tutto l'orario di lavoro e comunque coerentemente alla posizione organizzativa ricoperta dell'interessato.

Per ulteriori approfondimenti, si fa riferimento alla specifica policy sui dispositivi mobili di cui al capitolo 6 della presente policy.

4.16 Apparecchiature di riproduzione/registrazione immagini

L'utilizzo di apparecchiature aziendali di riproduzione/registrazione immagini è consentito previa autorizzazione del responsabile di struttura solo ed esclusivamente per ragioni tecniche e strettamente legate all'attività lavorativa; le immagini ottenute possono essere divulgate all'interno e/o all'esterno, previa autorizzazione della direzione aziendale -e in modo conforme con le direttive da essa impartire- conformemente con quanto previsto dal Regolamento Europeo 679/2016. Tali principi hanno l'obiettivo di tutelare la riservatezza dei dati personali trattati e dell'integrità del patrimonio aziendale.

È vietata l'esecuzione di riproduzione/registrazione di immagini, a qualsiasi titolo, con apparecchiature personali o di terzi, se non espressamente autorizzati dalla Direzione Aziendale.

Non è consentito l'utilizzo di sistemi di videoconferenza/audioconferenza se non preventivamente autorizzati dalla struttura T.I. - sussistendo il grave pericolo di introdurre codice malevolo e/o di alterare la funzionalità delle applicazioni software esistenti.

4.16.1 Microsoft Teams

ARCS, per agevolare i dipendenti che dovessero beneficiare dell'istituto dello *Smart Working* e per favorire la comunicazione con fornitori e soggetti esterni, ha introdotto la piattaforma Microsoft Teams quale strumento di collaborazione digitale.

Poiché tale piattaforma permette la registrazione delle riunioni, l'Azienda ha istituito la seguente procedura per registrare gli eventi in modalità conforme alla normativa privacy.

4.16.1.1 Registrazione eventi di Microsoft Teams

È consentito registrare esclusivamente gli eventi inquadrati come "formativi" (lezione frontale, addestramento, work-on-the-job, informazione, ecc.); qualsivoglia differente situazione -gruppo di

lavoro, riunione interna di struttura, incontro sindacale, collegio, OIV, ecc.- dovrà ricevere specifica e formale autorizzazione della direzione aziendale.

La registrazione dell'evento prevede che l'organizzatore della riunione notifichi la modalità di "evento registrato" già all'atto della trasmissione della convocazione/invito. Avviata la registrazione i partecipanti vedranno comparire nella sezione superiore del proprio client un banner che segnala la registrazione in corso "La registrazione è stata avviata. È in corso la registrazione della riunione. Partecipando, fornisci il tuo consenso alla registrazione della riunione. Clicca qui per l'informativa sulla privacy". Oltre alla segnalazione nel banner, l'organizzatore dell'evento deve avvisare i partecipanti espressamente e prima dell'inizio che la seduta verrà registrata. Qualora un partecipante non acconsentisse alla registrazione dev'essere invitato a tenere microfono e telecamera disattivati e intervenire, eventualmente, solo tramite chat.

Con specifico riferimento ai i docenti, l'organizzatore dell'incontro deve assicurarsi che il relatore sottoscriva una specifica liberatoria ad hoc -disponibile presso la formazione aziendale ARCS- per l'utilizzo di registrazioni ed immagini in relazione al diritto d'autore sui contenuti.

Per gli eventi non inquadrati come "formativi", sempre in virtù dei principi di limitazione delle finalità di trattamento e minimizzazione dei dati, è permessa la registrazione dell'incontro limitatamente a quei casi ove questo risulta particolarmente utile o necessario per l'attività, ma esclusivamente previa autorizzazione della Direzione. Rimane comunque necessario acquisire il consenso espresso di tutti i partecipanti da rendere al momento della registrazione stessa (senza liberatorie). Nel caso in cui il consenso venga negato da uno o più soggetti si può applicare la medesima regola dei corsi di formazione, ovvero si invitano tali partecipanti a spegnere microfono e telecamera e a comunicare solo tramite chat (se l'intervento dei soggetti che si oppongono alla registrazione risulta invece indispensabile, la registrazione non potrà essere effettuata).

Resta onere dell'organizzatore provvedere alla puntuale cancellazione delle registrazioni tenuto conto del "principio di minimizzazione" dettato dal GDPR secondo il quale i dati debbono essere: adeguati, pertinenti e *limitati a quanto necessario rispetto alle finalità per le quali sono trattati*.

Ogni struttura, eccezione fatta per il Centro Regionale Formazione, può richiedere al più l'abilitazione di un singolo operatore; tecnicamente, l'abilitazione delle utenze alla registrazione degli eventi, può richiedere delle tempistiche di allineamento dei sistemi fino a 96 ore.

4.17 Utilizzo di stampanti, multifunzioni e fax-server

È vietato l'utilizzo delle stampanti, delle fotocopiatrici (MF) e dei Fax aziendali per fini personali.

In alcune sedi lavorative dell'Azienda è stato introdotto un nuovo sistema di stampa distribuito per incrementare l'efficienza nell'uso dei disposi (ottimizzazione e controllo dell'uso delle multifunzioni) e l'utilizzo di servizi avanzati (es. follow me printing e secure printing).

La stampa di documenti informatici dovrà essere limitata ai casi per cui esiste l'assoluta necessità di disporre della copia cartacea.

Il materiale stampato deve essere immediatamente prelevato per evitare che possa essere visionato da personale non autorizzato.

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).

4.18 Responsabilità e doveri relativi alla sicurezza delle informazioni

Al fine di tutelare il patrimonio informativo aziendale, i dati e le informazioni in esso contenuti, si invitano tutti i dipendenti a segnalare alla struttura T.I. eventuali criticità e punti deboli del sistema informativo (o in senso generale eventi) o comportamenti anomali dei sistemi.

In particolare, se il dipendente sospetta che un qualsiasi computer o supporto esterno (chiavette USB, CD/DVD, ecc…) sia affetto da virus deve immediatamente informare la struttura T.I. attraverso comunicazione scritta e/o segnalazione formalizzata evitando di segnalare a soggetti terzi o di intervenire personalmente.

4.19 Sistemi di controlli graduali e verifiche

L'ARCS 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 della struttura T.I. (o Insiel S.p.A. per conto del rapporto in essere con l'Azienda)

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.

4.19.1 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. Per maggiori informazioni si rimanda al Decreto ARCS "AMMINISTRATORI DI SISTEMA" n.189 del 26.08.2020

4.19.2 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. ARCS 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.

ARCS 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 particolare, 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 e automaticamente, 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.

4.19.3 Posta elettronica ordinaria (PEO)

ARCS adotta le seguenti soluzioni che consentano comunque lo svolgimento della regolare attività lavorativa, sia che l'uso della PEO avvenga tramite dispositivi aziendali o personali:

- condivisione di indirizzi di posta elettronica tra più lavoratori, tramite la creazione di caselle di posta di servizio non personali;
- 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;
- 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, ARCS 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 tramite il responsabile di struttura (o suo delegato);
- 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;

4.19.4 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.

ARCS 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.

5 Dispositivi cellulari

5.1 Politiche di accesso ai dati

Concedere l'accesso a dati aggiornati in tempo reale ai dipendenti in remoto e fornire loro la possibilità di caricare informazioni sui sistemi aziendali può portare ad un aumento dell'efficienza aziendale e dell'immediatezza.

Oltre ai significativi vantaggi, però, bisogna affrontare anche alcune problematiche per far sì che l'iniziativa di accesso tramite dispositivi mobili non vada a minare la sicurezza dei sistemi e dei dati, o non porti l'azienda a non rispettare le normative o le esigenze di conformità esistenti.

Per questo motivo l'accesso ai dati attraverso l'uso dei dispositivi cellulari può avvenire sulla base delle indicazioni legate alla classificazione dei dati; di seguito quindi si identificheranno le seguenti tipologie di dispositivi:

- dispositivo gestito: dispositivo sul quale è stato installato un software MDM fornito dall'Azienda;
- dispositivo verificato: dispositivo su cui è stata configurata la posta elettronica tramite protocollo ActiveSync, ma non un software MDM;
- dispositivo non gestito/verificato: dispositivo (generalmente personale, ossia di proprietà dell'utente quali smartphone o tablet) su cui non è stato installato un software MDM né è stata configurata la posta elettronica aziendale tramite protocollo ActiveSync.

	Dati pubblici e personali	Particolari categorie di dati personali (ex sensibili) o dati riservati
Dispositivo gestito	✓	✓ (in conformità alle politiche di sicurezza definite di seguito)
Dispositivo verificato	✓	×
Dispositivo non gestito/verificato	×	×

Fino all'introduzione di un software MDM a livello aziendale, i dispositivi verificati saranno assimilati ai dispostivi gestiti.

Nel caso di accesso da dispositivo gestito/verificato a dati sensibili e/o riservati devono essere rispettate le seguenti politiche:

- il canale di comunicazione deve essere crittografato (ad esempio tramite HTTPS);
- non è permesso all'utente salvare i dati sul dispositivo.

L'uso del dispositivo deve rispettare le regole obbligatorie descritte nel capitolo successivo REGOLE PER LA GESTIONE E L'UTILIZZO DEI DISPOSITIVI CELLULARI.

L'utente è informato che, sia nel caso di utilizzo di dispositivi personali che aziendali per la gestione della casella di posta aziendale 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).

5.2 Regole per la gestione e l'utilizzo dei dispositivi cellulari

L'uso dei dispositivi cellulari deve seguire le politiche e le regole di sicurezza stabilite dall'Azienda; viene inoltre indicata, per ogni regola, la tipologia di dispositivo cellulare applicabile:

- personale (verificato o gestito)
- aziendale

5.2.1 Software/Hardware

Applicabilità: Cellulari aziendali e personali

Tutti i cellulari forniti dall'Azienda ai propri dipendenti devono essere registrati e controllati centralmente dal sistema MDM in dotazione all'azienda (rendendoli "dispositivi gestiti") oppure configurati con la posta elettronica aziendale tramite protocollo *ActiveSync* (rendendoli "dispositivi verificati"). Eventuali dispositivi aziendali non gestiti o verificati dovranno essere consegnati alla struttura T.I. per una loro configurazione.

Non sono autorizzate modifiche hardware e software al dispositivo (come, ad esempio, jailbreaking su iPhone oppure rooting su Android).

I software dei dispositivi devono essere aggiornati. Gli aggiornamenti devono essere controllati ogni settimana e applicati almeno una volta al mese a cura del dipendente.

5.2.2 Accesso ai dispositivi

Applicabilità: Cellulari aziendali e personali

Dovrà essere garantita la protezione dei dati, configurando l'accesso dei dispositivi mobili in maniera sicura. Per tale motivo è previsto l'utilizzo di un pin o di una password ed il blocco dello schermo dei dispositivi mobili. I dispositivi devono essere configurati con un pin o una password sicura, diversa dalle altre utilizzate all'interno dell'azienda.

Per una corretta gestione della sicurezza, analogamente, il telefono sarà predisposto in modo che per sbloccare il telefono da standby venga utilizzato il lettore di impronta digitale o il codice precedentemente impostato. Quando un dipendente ritiene che sia avvenuto un accesso non autorizzato ai dati aziendali tramite un dispositivo mobile, dovrà segnalare l'incidente in conformità con il processo di gestione degli incidenti vigente.

5.2.3 Applicazioni

Applicabilità: Cellulari aziendali e personali

Il dipendente potrà installare soltanto applicazioni provenienti dai repository ufficiali dei fornitori dei dispositivi mobili (es. Google Play, Apple ITunes), firmate digitalmente, nonché formalmente approvate dalla struttura T.I.

Sono vietate tutte le applicazioni il cui utilizzo può arrecare danni di reputazione o economici, nonché l'uso di programmi che violino la normativa nazionale e internazionale. Di seguito viene riportato un elenco, non esaustivo, delle categorie di applicazioni vietate:

- pornografia;
- crittografia dei dati (se diversa da quella fornita dalla società);
- anonimizzatori;
- condivisione di materiale coperto da copyright;
- strumenti di rilevazione e attacco dei sistemi (es. port scanning);
- intercettazione e registrazione delle comunicazioni.

Nel caso in cui si utilizzi un dispositivo personale con all'interno la posta elettronica configurata tramite protocollo *ActiveSync*, il dipendente si atterrà alle disposizioni in materia di BYOD, in particolare al requisito **REQ-SIC-BYOD-02a**.

5.2.4 Reti telematiche

Applicabilità: Cellulari aziendali e personali

Gli utenti finali non dovranno utilizzare reti telematiche insicure per la trasmissione dati, come ad esempio le reti Wi-Fi non protette da password, o protette da meccanismi deboli (ad esempio, WEP). Le reti configurate con meccanismi di protezione deboli permettono l'intercettazione delle informazioni inviate con conseguente privazione della riservatezza e dell'integrità dei dati.

5.2.5 Informazioni archiviate

Applicabilità: Cellulari aziendali e personali

I dipendenti non hanno il permesso di memorizzare le password in modo non cifrato sul proprio dispositivo.

Inoltre, nessun utente finale è autorizzato a copiare o inserire dati dell'Azienda sul dispositivo o sulla scheda di memoria rimovibile, a meno che i dati siano crittografati.

5.2.6 Smarrimento o furto

Applicabilità: Cellulari personali

In caso di furto o smarrimento deve essere immediatamente informata la struttura TI in modo da minimizzare il rischio di sottrazione di dati tramite le procedure in precedenza descritte.

Applicabilità: Cellulari aziendali

In caso di furto o smarrimento deve essere immediatamente informata la struttura TI in modo da bloccare remotamente il telefono; deve essere inoltre fornita in copia la denuncia presentata presso gli organi competenti (carabinieri, polizia).

ARCS ha facoltà, in caso si ravvedesse una negligenza da parte dell'utente, di trattenere a titolo risarcitorio -mediante ritenuta in busta paga- l'importo che verrà richiesto dal proprietario del bene.

5.2.7 Riutilizzo e dismissione

Applicabilità: cellulari aziendali

In caso di dismissione del dispositivo o di riassegnazione ad altro dipendente, deve essere realizzata la cancellazione sicura delle informazioni per proteggere le informazioni riservate e i dati personali secondo la normativa sulla privacy. Contattare il SOC, al momento della redazione del presente documento ruolo ricoperto dalla struttura T.I., per poter eseguire il wiping dei dati.

5.2.8 Regole comportamentali

Applicabilità: cellulari aziendali e personali

Oltre alle disposizioni già elencate nella sezione UTILIZZI CONSENTITI, i dipendenti devono utilizzare particolari accortezze nell'uso dei dispositivi cellulari nei luoghi pubblici, nelle sale riunioni e in qualsiasi altra area non sicura per evitare accessi non autorizzati o divulgazione involontaria di informazioni.

I dispositivi cellulari devono anche essere protetti fisicamente da furto, quindi, non devono essere lasciati dentro i veicoli, nelle stanze di hotel, ecc... I dispositivi, specialmente quelli contenenti informazioni sensibili, non devono mai essere lasciati incustoditi e, laddove possibile, devono essere tenuti in posti sicuri chiusi a chiave.

5.2.9 Bring Your Own Device (BYOD)

Applicabilità: cellulari personali

Con il termine BYOD si intende l'utilizzo, da parte del personale, dei propri dispositivi mobili per accedere alle reti e ai contenuti di proprietà dell'azienda.

L'uso di dispositivi personali introduce dei rischi di sicurezza. Il fattore di maggior problematicità è rappresentato dall'utilizzo promiscuo e per finalità differenti -lavorative e personali- dei dispositivi mobili da parte dei lavoratori.

Analizzando il concetto in ottica privacy e protezione dei dati personali, la conseguenza inevitabile è che il dipendente/lavoratore gestisce ed utilizza per fini aziendali il dispositivo di sua stessa proprietà, mentre il datore di lavoro è il soggetto obbligato a conformarsi alle prescrizioni e a ogni altro obbligo previsto dalla normativa in materia di protezione dei dati personali.

Nello stabilire la policy di sicurezza relativamente al contesto BYOD, come chiarito dall'Information Commissioner's Office -la prima Autorità europea per la protezione dei dati personali ad aver emanato delle linee guida BYOD in merito- è essenziale considerare, in ottica preventiva, i seguenti aspetti:

- la tipologia e la natura dei dati trattati;
- il luogo di conservazione dei dati;
- le modalità di trasferimento e il flusso dei dati;
- le possibilità di perdita/alterazione dei dati;
- il livello di commistione/promiscuità tra finalità personali e aziendali nei trattamenti dei dati;
- il livello di sicurezza dei singoli dispositivi mobili;
- gli effetti di una potenziale conclusione del rapporto lavorativo tra Impresa e lavoratore;
- le modalità di gestione di eventuali perdite, furti, malfunzionamenti e/o rotture di un dispositivo.

In questo contesto si stabilisce quanto segue:

Codice	Comportamento applicato
REQ-SIC-BYOD-01	I dipendenti accedono ai servizi della intranet, alla VPN, alle applicazioni client e mobile della posta elettronica ed alle altre risorse IT della rete interna solo tramite dispositivi (smartphone, tablet, laptop e desktop) forniti dall'azienda in dotazione.
REQ-SIC-BYOD-02	È data facoltà ai dipendenti di poter configurare sui propri dispositivi cellulari personali la posta elettronica, esclusivamente tramite protocollo *ActiveSync.* In tal caso il dipende deve adeguarsi alle disposizioni fissate nella presente policy
REQ-SIC-BYOD-02a	Nel caso in cui il dispositivo personale venisse *verificato*, è fatto d'obbligo al dipendente di installare soltanto applicazioni provenienti dai repository ufficiali dei fornitori dei dispositivi mobili (es. Google Play, Apple ITunes), firmate digitalmente
REQ-SIC-BYOD-03	L'Azienda mette a disposizione degli ospiti e dei frequentatori occasionali di alcune aree aziendali, reti wireless per l'accesso a internet (wifi "*ARCS-ospiti*")
REQ-SIC-BYOD-04	Le reti ospiti sono separate dalle reti aziendali (che permettono l'accesso ai servizi).
REQ-SIC-BYOD-05	Per l'accesso a tali reti, appunto perché non interconnesse a quelle aziendali, è permesso l'utilizzo di dispositivi personali.
REQ-SIC-BYOD-06	Nel caso di reti interconnesse ai servizi IT interni, sia che si tratti di reti fisiche che di reti wireless, i dipendenti non sono autorizzati all'utilizzo dei dispositivi personali.

Codice	Comportamento applicato
REQ-SIC-BYOD-07	Nell'ambito delle forniture di servizi IT, o altre situazioni assimilabili, che prevedano la presenza di personale esterno, l'accesso alle reti fisiche o wireless interconnesse ai servizi IT, per motivi di servizio, è autorizzato in presenza di clausole contrattuali o accordi scritti e formalizzati.
REQ-SIC-BYOD-08	Nel caso del [REQ-SIC-BYOD-07] la ditta erogatrice dei servizi è responsabile della conformità dei dispositivi alle normative ed alle politiche di sicurezza.
REQ-SIC-BYOD-09	È d'obbligo applicare misure di sicurezza adeguate e congrue (tra cui in primis la separazione tra le reti adibite agli utenti ospiti occasionali e le reti che permettano accesso ai dati), atte ad impedire alla fonte comportamenti non conformi a quanto esposto.
REQ-SIC-BYOD-10	È d'obbligo l'osservanza da parte dei dipendenti, dei fornitori esterni e degli ospiti occasionali le politiche in tema di accesso alla rete e utilizzo dei dispositivi, e in generale il rispetto delle politiche di sicurezza e, laddove previsto, delle clausole contrattuali.

6 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 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 protetto da Firewall gestito da Insiel S.p.A.

L'abilitazione e le credenziali di accesso vengono forniti dal personale della struttura T.I.- 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 Arcs in unità organizzative (OU) preposte.

7 Notifiche di Non-conformità, misure disciplinari e aggiornamenti alla politica

Dipendenti, collaboratori e soggetti terzi equiparabili a Personale interno dell'Azienda sono tenuti a rispettare la presente policy e le altre politiche pubblicate.

Il mancato rispetto o la violazione delle regole contenute in questa policy, 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.

Il personale incaricato deve valutare qualsiasi eccezione dall'osservanza di particolari disposizioni contenute nella presente policy e nelle altre politiche pubblicate. Le deroghe rilasciate di volta in volta saranno prese in considerazione solo se circostanze speciali non consentono l'attuazione pratica di un requisito, se una legge o un regolamento locale o regionale supporta un'esenzione richiesta e se sono in atto controlli compensativi per ridurre il rischio di non conformità.

Questa politica, proposta dal dirigente della struttura T.I., 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'Azienda.

Il mantenimento, l'aggiornamento e qualsiasi modifica della presente policy è assoggettato alla verifica e successiva approvazione della Direzione in coerenza alle disposizioni del GDPR e dei processi organizzativi dell'Azienda.

È fatto obbligo di adeguare i propri comportamenti alle disposizioni previste nella presente policy ed a chiunque competa di osservarla.

8 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 sopra richiamate, qualora siano ravvisabili profili quantomeno colposi nella condotta osservata, è perseguibile nei confronti del personale dipendente con i provvedimenti disciplinari e risarcitori previsti dalla normativa applicabile.

9 Terminologia e abbreviazioni

Termine	*Definizione*
AirCard	l'AirCard è un modem wireless che permette di collegare qualsiasi dispositivo ad Internet, utilizzando la connessione dati di un cellulare.
AOO	Aree Organizzative Omogenee, identificano gli uffici di protocollo degli Enti che gestiscono i flussi documentali in entrata ed in uscita dall'Ente
Autenticazione informatica	l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità
Banca dati	qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti
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
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
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
DCSISPS	Direzione centrale salute, integrazione sociosanitaria e politiche sociale
DHCP	Dynamic Host Configuration Protocol, è un Protocollo Applicativo che permette ai dispositivi di una certa rete locale di ricevere automaticamente ad ogni richiesta di accesso, da una rete IP (LAN), la configurazione IP necessaria per stabilire una connessione e operare su una rete più ampia basata su Internet Protocol

Termine	*Definizione*
Disponibilità	Requisito di sicurezza in base al quale un'informazione deve essere accessibile e utilizzabile su richiesta dai soggetti autorizzati.
DNS	Domain Name System, è un sistema utilizzato per assegnare nomi ai nodi della rete
GPS	Global Positioning System è un sistema di posizionamento e navigazione satellitare civile
GSM	Global System for Mobile è lo standard 2G (2ª generazione) di telefonia mobile cellulare
Hardware	indica la parte fisica di un computer, ovvero tutte quelle parti elettroniche, elettriche, meccaniche, magnetiche, ottiche che ne consentono il funzionamento (dette anche strumentario)
Incaricati	le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal ò
INSIEL	Informatica per il Sistema di 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
Integrità	requisito di sicurezza in base al quale un'informazione deve essere accurata e completa.
Interessato	persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali
IP	Internet Protocol, è un'etichetta numerica che identifica univocamente un dispositivo collegata ad una rete informatica (protocollo di comunicazione). Un indirizzo IP assolve due funzioni principali: identificare un dispositivo sulla rete e, di conseguenza, fornire il percorso per la sua raggiungibilità da un altro terminale o dispositivo di rete. Può essere statico (configurato manualmente) o dinamico (configurato automaticamente)
Jailbreaking	procedura che permette di eludere la verifica del codice da eseguire che è posta in essere ad ogni accensione o riavvio del dispositivo Apple (iBoot).
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…
Laptop	Personal Computer portatile
MDM – Mobile Device Management	Mobile Device Management, strumento o software progettato per aiutare gli amministratori IT a controllare e proteggere i dispositivi mobile, come smartphone e tablet, all'interno di un'organizzazione. L'MDM è una parte importante dell'enterprise mobility management e della gestione degli endpoint, specialmente alla luce della crescita del numero di aziende che adottano politiche di bring your own device

Termine	*Definizione*
	(BYOD) che consentono ai dipendenti di accedere ai dati aziendali, ai file e alle applicazioni sui propri dispositivi personali.
MiFi	MiFi è una tecnologia che consente agli utenti finali e dispositivi mobili di condividere una connessione a banda larga mobile a Internet 3G o 4G e creare una rete ad-hoc.
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
NTP	Network Time Protocol, è un protocollo per sincronizzare gli orologi dei computer all'interno di una rete a commutazione di pacchetto
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
PEC	Posta Elettronica Certificata
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	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
Riservatezza	Requisito di sicurezza in base al quale un'informazione non deve essere disponibile o divulgata a soggetti non autorizzati.
Rooting	Procedura di rooting permette di abilitare l'utilizzo dell'account root e quindi acquisire privilegi amministrativi.
SSID	Service Set IDentifier, nome con cui una rete senza fili si identifica ai suoi utenti
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
SOC	Security Operations Center. Centro da cui vengono forniti servizi finalizzati alla sicurezza dei sistemi informativi
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

Termine	*Definizione*
	programmi, oppure da uno o più dati, oppure da una combinazione delle due
Split Tunnel	Modalità di funzionamento della VPN per cui solo determinato traffico viene instradato all'interno della VPN
Spyware	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
T.I.	struttura semplice dipartimentale "T.I."
Titolare del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri
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	nome/identificativo con il quale l'utente viene riconosciuto da un computer, da un programma o da un server
Utente	ciascuna persona che accede alle risorse informatiche aziendali

Termine	*Definizione*
VPN	Virtual Private Network, canale cifrato fra due dispositivi che permette di scambiare dati riservati all'interno di un canale non sicuro (ad es. Internet)
Web Filtering	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
Web Security	consiste nel monitoraggio di tutte le informazioni sul traffico Internet
WEP	Wired Equivalent Privacy: tecnica di crittografia dei dati per rendere sicure le trasmissioni radio delle reti Wi-Fi. Tale algoritmo si è dimostrato vulnerabile e quindi se ne sconsiglia l'uso.
WiFi	WiFi è una tecnologia che consente agli utenti finali e dispositivi mobili di collegarsi tra loro attraverso una rete locale senza fili (WLAN)
Wiping	cancellazione sicura dei dati
Worm	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
WWW	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)

10 Modello di concessione in uso e consegna

Con la presente l'Azienda Regionale di Coordinamento per la Salute

CONCEDE IN USO E CONSEGNA

al Sig. _____, incardinato presso la struttura _____, i seguenti dispositivi:

Tipologia assegnamento	□ dispositivo personale □ dispositivo struttura
PC marca, modello e cespite:	
Monitor:	
Webcam:	
Cuffie:	
Dispositivo di memoria esterno/Chiavetta USB:	

Gli asset aziendali sono consegnati alle seguenti condizioni:

a) l'utilizzo si intende autorizzato per l'intera durata del rapporto lavorativo;
b) i beni sopra descritti debbono servire per adempiere alle mansioni lavorative assegnate;
c) l'utente si obbliga come previsto dal Codice Penale e dal "Codice di comportamento di ARCS":
   - a conservare e a custodire i beni in oggetto con la massima cura e diligenza cura e massima diligenza;
   - a non destinare i beni in oggetto ad altri usi che non siano quelli sopra previsti inerenti all'attività lavorativa;
   - a non cedere neppure temporaneamente (a meno di dispositivi assegnati a livello di struttura) l'uso dei beni sopra individuati a terzi, né a titolo gratuito né a titolo oneroso;
   - a restituire i beni stessi nello stato attuale in cui si trovano -fatto salvo il normale deterioramento d'uso- in qualsiasi momento su richiesta di ARCS e, in ogni caso, entro la fine del rapporto lavorativo di cui alla lett. a);
d) sono a carico di ARCS gli oneri di riparazione e le spese derivanti dall'utilizzo dei suddetti beni ad eccezione delle spese eventualmente derivanti da danni causati da dolo dell'utente;
e) i dispositivi sono da considerarsi uno strumento informatico aziendale ed in quanto tale rientrano nel "*Regolamento del corretto utilizzo degli strumenti informatici*", noto all'utente e che con la sottoscrizione del presente verbale ne conferma la conoscenza anche sotto il profilo del corretto trattamento dei dati personali derivante dall'utilizzo dello strumento stesso;
f) in caso di furto o smarrimento deve essere immediatamente informata la direzione in modo da bloccare remotamente il dispositivo smarrito/rubato. In caso di furto deve essere inoltre fornita in copia all'azienda la denuncia presso gli organi competenti (carabinieri, polizia): qualora non vengano rispettate le presenti disposizioni non sarà garantita alcuna sostituzione del bene;
g) qualora lo smarrimento/furto di un dispositivo fosse addebitabile alla condotta negligente posta in essere dall'utente, l'ARCS si riserva la facoltà di trattenere a titolo di risarcimento, mediante ritenuta in busta paga, l'importo richiesto per il reintegro del bene;
h) ARCS si riserva altresì la facoltà di chiedere il risarcimento in caso di danno causato al bene intenzionalmente e/o per colpa dell'utente;
i) nel caso di assegnazione di dispositivo di memoria esterno (USB), l'uso è autorizzato esclusivamente se:
   - il device è stato preventivamente cifrato con tecnologia Bitlocker (tassativamente a cura della struttura Tecnologie Informatiche);
   - l'utente si obbliga a non scaricare (copiare/spostare) i file contenuti nella memoria USB, su dispositivi (PdL, laptop, ecc …) diversi da quelli aziendali ARCS;

- l'utente si impegna a non diffondere né comunicare a terzi per alcuna ragione la chiave di cifratura, a conservarla in luogo protetto - separato dal dispositivo stesso- e a non modificare la stessa senza previa ed esplicita autorizzazione della struttura Tecnologie Informatiche;

j) si rammenta infine che eventuali violazioni alle disposizioni di cui al presente modulo - causate da inosservanza colposa o dolosa dell'utente - potranno essere soggette a sanzioni disciplinari.

Letto, approvato e sottoscritto

Udine, il _____

_____
Firma dell'assegnatario

Riconsegna

Con la presente, l'incaricato della struttura Tecnologie Informatiche riceve dal sig. _____, il materiale sopra individuato in stato funzionante e con i normali segni di usura dovuti all'uso.

_____
Nome e Cognome Incaricato T.I.

Udine, il _____

_____
Firma incaricato T.I.