

Policy per l'assegnazione e l'utilizzo dei dispositivi di telefonia mobile di servizio

MATRICE DELLE REVISIONI

REVISIONE	DATA	DESCRIZIONE / TIPO MODIFICA	REDATTA DA	VERIFICATA DA	APPROVATA DA
00	02/03/2022	Emissione	Nicola Bortolotti	Fabio Buffolini Riccardo-Mario Paoli	Joseph Polimeni
01					
02					
03					
04					
05					
06					

SOMMARIO

1	Premessa.....	3
2	Ambito di applicazione	3
3	Concessione dei telefoni cellulari di servizio	3
4	Contesto di riferimento	4
5	Classificazione dei dispositivi mobili	4
5.1	Dispositivi mobili ad uso esclusivo	5
5.2	Dispositivi mobili ad uso struttura.....	5
5.3	Dispositivi mobili ad uso allarmistica.....	6
6	Richiesta dispositivi mobili.....	6
7	Presa in carico.....	6
8	Disposizioni per l'utilizzo dei dispositivi	7
9	Attivazione/Assegnazione utenza telefonica.....	8
10	Sostituzione del dispositivo mobile.....	8
10.1	Guasti e malfunzionamenti.....	8
10.2	Furto e smarrimento	9
11	Cessazione/Restituzione/Riassegnazione/Riscatto	9
12	Disponibilità.....	10
13	Attivazione servizi opzionali.....	11
13.1	Servizio "Dual Billing-Tim Tuo"	11
13.2	Servizio "Tim Tuo Roaming On Extra Spazio Economico Europeo"	11
14	Politiche di accesso ai dati ARCS.....	11
15	Regole per la gestione e l'utilizzo dei dispositivi gestiti o verificati.....	13
15.1	Software/Hardware.....	13
15.2	Accesso ai dispositivi mobili.....	13
15.3	Applicazioni	13
15.4	Reti telematiche	14
15.5	Informazioni archiviate (per dispositivi verificati)	14
15.6	Regole comportamentali.....	14
15.7	Bring Your Own Device (BYOD)	14
16	Trattamento dei dati personali.....	16
17	Disposizioni finali, entrata in vigore e pubblicità	16
18	Notifiche di non-conformità, misure disciplinari e aggiornamenti alla politica	17
19	Terminologia e abbreviazioni	17
20	Allegati.....	20

1 PREMESSA

La presente policy ha per oggetto la disciplina relativa all'uso dei telefoni cellulari di servizio e degli strumenti per la connettività dati da rete mobile. Tale scopo viene ottenuto:

- definendo i criteri per l'assegnazione dei dispositivi di telefonia mobile ARCS;
- disciplinando l'utilizzo dei dispositivi di telefonia mobile di proprietà e/o gestiti da ARCS e dei relativi servizi erogati;
- stabilendo le norme comportamentali valide per tutti i soggetti che, a qualunque titolo, abbiano in affidamento i sopracitati dispositivi.

2 AMBITO DI APPLICAZIONE

La policy si applica a tutto il personale dipendente, senza distinzione di ruolo e/o livello che utilizza la telefonia mobile ARCS. Ha la finalità di illustrare le regole generali di assegnazione e di utilizzo dell'utenza mobile, dei dispositivi di telefonia e dei servizi di *dual billing* (utilizzo del cellulare ARCS per uso personale), nonché le modalità operative da seguire in caso di sostituzione del dispositivo.

3 CONCESSIONE DEI TELEFONI CELLULARI DI SERVIZIO

Al personale dipendente possono essere assegnati cellulari di servizio o strumenti per la connettività da rete mobile in base ad uno o più dei seguenti criteri:

1. *adempimenti necessari per attuare obblighi di pubblico interesse*: soggetti i cui adempimenti richiedono oggettivamente il possesso del dispositivo mobile per finalità di servizio (ad esempio, il personale che deve accreditarsi alla piattaforma della Banca Dati Nazionale unica per la documentazione Antimafia -B.D.N.A.- o i dispositivi richiesti per la gestione degli accessi al portale Consip);
2. *utenze ad uso allarmistica*: vedi successiva sezione 5 "classificazione dei dispositivi mobili";
3. *utenze ad uso struttura*: vedi successiva sezione 5 "classificazione dei dispositivi mobili";
4. *utenze afferenti alla segreteria di direzione preventivante individuate dalla direzione strategica*;
5. *responsabili di struttura semplice (SS), semplice dipartimentale (SSD) e complessa (SC)* i quali dovranno mettersi nelle condizioni di ricevere le chiamate, a meno di assenza dal servizio, dalle ore 8:00 alle ore 18:00. Resta facoltà del dipendente rendersi raggiungibile anche nei periodi di assenza dal servizio.

Tutte le richieste che non rientrano nelle casistiche in precedenza elencate (quando ad esempio la natura delle prestazioni e dell'incarico richiedono pronta e costante reperibilità in luoghi diversi dalla sede di lavoro, quando sussistono particolari e indifferibili esigenze di comunicazione che non possono essere soddisfatte con gli strumenti di telefonia e posta elettronica da postazione fissa ovvero in relazione a particolari forme di prestazione dell'attività lavorativa) dovranno essere adeguatamente motivate dal responsabile richiedente e saranno valutate dalla Direzione Amministrativa o da un soggetto da essi delegato.

Con riferimento ai possibili subentri di nuove utenze del personale proveniente da altre amministrazioni verso ARCS quale cessionario/subentrante (ad esempio in caso di mobilità in ingresso, comando o altre forme assimilabili), le utenze saranno prese in carico con le medesime modalità sopra descritte, ossia nei casi rispondenti ai criteri elencati oppure previa valutazione discrezionale della Direzione.

4 CONTESTO DI RIFERIMENTO

ARCS ha aderito alla convenzione CONSIP «*Telefonia mobile 8*», aggiudicata a Telecom Italia, per la fornitura del servizio di telefonia radiomobile allo scopo di effettuare telefonate di servizio, che prevede, in particolare, l'assegnazione di un telefono cellulare in comodato d'uso gratuito e l'attivazione di un'utenza di telefonia mobile con un piano tariffario a pacchetto.

Il telefono cellulare e l'utenza telefonica (SIM) sono a tutti gli effetti *strumenti di lavoro* in uso al dipendente.

L'utilizzo dei software aziendali impone che il dispositivo assegnato dovrà essere utilizzato esclusivamente con la SIM ARCS anche nel caso in cui il dispositivo consenta l'utilizzo di una seconda SIM (dual SIM). Attraverso la piattaforma amministrativa Mobile Device Management (MDM) Airwatch in uso presso ARCS e l'installazione sul telefono cellulare del software Workspace ONE di VMware, verranno gestite e configurate le policy di sicurezza, le applicazioni ad uso aziendale e protetti, attraverso cifratura, tutti i dati trattati.

Inoltre, in caso di furto, smarrimento o attacchi da codice malevolo, ARCS potrà bloccare e formattare il dispositivo cancellando i dati ivi contenuti. In ottemperanza a quanto previsto dalle norme dell'Unione Europea sul roaming a tariffa nazionale "*Roaming-like-at-home*", i servizi offerti compresi nel pacchetto sono utilizzabili anche in tutti i paesi dello Spazio Economico Europeo (per maggiori dettagli consultare la documentazione CONSIP).

L'uso dei dispositivi mobili deve seguire le politiche e le regole di sicurezza stabilite da ARCS di seguito al punto 14 della presente.

5 CLASSIFICAZIONE DEI DISPOSITIVI MOBILI

Per l'espletamento dell'attività lavorativa è prevista l'assegnazione al personale autorizzato di:

- un telefono cellulare in comodato d'uso gratuito corredato dei relativi accessori - caricabatteria, auricolari o altro- che dovranno essere utilizzati con diligenza e riconsegnati all'atto della restituzione del dispositivo;
- una carta SIM aziendale (disabilitata ai servizi Audiotel identificati dai prefissi 144, 166 e 199, agli SMS vs 488XXX, nonché all'accesso ai Servizi Premium), con un pacchetto di servizi per chiamate, SMS, MMS e traffico dati;

Ai soli fini del presente regolamento, i dispositivi mobili si suddividono in:

1. dispositivi mobili ad uso *esclusivo*,
2. dispositivi mobili ad uso *struttura*,
3. dispositivi mobili ad uso *allarmistica*.

5.1 Dispositivi mobili ad uso esclusivo

Comprendono i dispositivi mobili assegnati in via esclusiva all'assegnatario in relazione alla mansione svolta. Il dispositivo mobile ad uso esclusivo viene concesso a fronte di particolari posizioni nell'organizzazione che determinano la necessità di garantire costante raggiungibilità. I dispositivi mobili assegnati ad uso esclusivo non possono essere ceduti a terzi a nessun titolo. Nel caso di dispositivi mobili ad uso esclusivo l'utilizzatore corrisponde all'assegnatario.

5.2 Dispositivi mobili ad uso struttura

Comprendono i dispositivi mobili assegnati temporaneamente al personale di una struttura per il periodo necessario allo svolgimento delle attività che ne richiedono l'uso. Tali strumenti sono caratterizzati da alcune limitazioni: non è possibile, ad esempio, configurare una mail personale o installare alcune applicazioni (es. WhatsApp). Nel caso in cui un dispositivo mobile sia concesso ad uso struttura, la responsabilità dell'utilizzo dello stesso ricade sul Dirigente Responsabile della struttura stessa, che dovrà quindi, al fine di garantirne l'adeguata tracciabilità, assicurare l'annotazione delle seguenti informazioni nel **registro delle assegnazioni dei dispositivi mobili (Allegato 4)**:

- il nominativo dell'assegnatario;
- la data/ora di consegna del dispositivo e della relativa SIM;
- le esigenze di servizio;
- la data/ora di riconsegna dello stesso.

La creazione e l'aggiornamento di tale registro è in carico al Dirigente Responsabile che, in caso di richiesta dell'autorità competente, dovrà essere sempre in grado di fornire indicazioni relativamente alla persona che stava utilizzando il dispositivo e alle motivazioni per cui tale dispositivo era stato assegnato. In caso di mancata annotazione, l'utilizzatore corrisponderà al Dirigente Responsabile della struttura richiedente.

5.3 Dispositivi mobili ad uso allarmistica

Questo genere di dispositivi viene di norma fornito ed installato, comprensivo di SIM, dalla ditta individuata per la fornitura dell'impianto di allarme. In alcuni casi specifici la fornitura della SIM potrà essere effettuata, previa valutazione, direttamente dall'ARCS; in tal caso, la SIM verrà assegnata al Dirigente Responsabile del servizio che ha richiesto l'impianto. Lo stesso, dovrà fornire informazioni relativamente alle numerazioni da/verso cui la nuova utenza potrà effettuare il traffico fonia e SMS per chiamate di soccorso o segnalazioni di eventuali guasti e/o malfunzionamenti. Il Dirigente Responsabile dovrà inoltre tener traccia di dove sono state posizionate le SIM fornite ed avvisare il Gestore della Telefonia (GdT) qualora l'impianto non venga più utilizzato per la conseguente cessazione di tali utenze.

6 RICHIESTA DISPOSITIVI MOBILI

La richiesta inerente alla concessione in uso di nuove carte SIM, dispositivi mobili di servizio o modifiche alle configurazioni delle utenze esistenti, deve essere formalizzata ed indirizzata al GdT, utilizzando il modulo **Nuova richiesta di dispositivo telefonico mobile (Allegato 1)**

Il modello deve essere obbligatoriamente compilato in tutte le sue parti indicando nell'apposito spazio le motivazioni della richiesta.

La richiesta deve essere firmata digitalmente dal Dirigente Responsabile della Struttura richiedente ed autorizzata, con sottoscrizione digitale, dal direttore di Dipartimento al quale la struttura afferisce.

Il GdT verifica che la modulistica sia redatta in ogni sua parte, integrata dalle motivazioni che hanno spinto ad effettuare la richiesta ed autorizzata. In seguito, precederà all'approvvigionamento e alla consegna del dispositivo e/o SIM aggiornando la documentazione tecnico/amministrativa che conterrà le seguenti informazioni:

- informazioni relative all'utenza numero telefonico e data di attivazione della SIM;
- informazioni relative alla concessione in uso quali la struttura di appartenenza, e, nel caso di concessione ad uso esclusivo nome e cognome dell'assegnatario;
- informazioni sull'apparecchio utilizzato quali marca, modello, IMEI (n. identificativo)

7 PRESA IN CARICO

Per la presa in carico delle carte SIM, degli apparati e degli accessori di telefonia mobile dovrà essere firmato l'apposito modulo **Presa in carico dispositivo telefonico aziendale (Allegato 2)** contenente la descrizione dei beni.

La firma apposta su tale modulo, costituisce accettazione integrale della presente policy e la conseguente assunzione di responsabilità; la sottoscrizione dovrà essere apposta dal diretto

assegnatario in caso di dispositivo mobile ad uso esclusivo, o dal Dirigente Responsabile della struttura richiedente in caso di dispositivo mobile ad uso struttura.

Qualora le figure indicate fossero impossibilitate al ritiro del dispositivo (o della SIM) potranno individuare un delegato previa compilazione del modulo **Delega per presa in carico dispositivo telefonico aziendale (Allegato 3)**

8 DISPOSIZIONI PER L'UTILIZZO DEI DISPOSITIVI

Nell'utilizzo del dispositivo mobile, il dipendente deve adottare un comportamento conforme a quanto previsto da CCNL, Codice di comportamento aziendale, GDPR, dalla Policy per il corretto utilizzo degli strumenti informatici e dal vigente PIAO – Sezione Organizzazione e Capitale Umano.

Tutti i dispositivi mobili devono essere utilizzati, da parte degli utenti, in modo strettamente pertinente alla propria attività lavorativa o carica istituzionale; gli utenti stessi devono impegnarsi per un utilizzo appropriato, efficiente, corretto e razionale. L'effettuazione delle chiamate deve rispondere a criteri di effettiva necessità ed urgenza. La durata delle chiamate deve essere la più breve possibile in relazione alle esigenze di servizio. Gli utenti dovranno utilizzare il dispositivo mobile nei casi di effettiva necessità, ponendo la massima attenzione al contenimento della spesa.

I dispositivi di telefonia mobile possono essere utilizzati soltanto per ragioni di servizio e viene fatto divieto tassativo di effettuare chiamate personali o per scopi diversi da quello di servizio. L'uso ai fini privati delle apparecchiature potrà avvenire solo in caso di contratto *dual billing* previa attivazione del servizio (*vedi attivazione servizi opzionali*).

Qualsiasi modifica alla configurazione hardware e software del dispositivo è vietata e ricade sotto la diretta responsabilità dell'assegnatario.

Il Dipendente è inoltre tenuto a:

- utilizzare la SIM assegnata esclusivamente con il dispositivo mobile messo a disposizione di ARCS (e non con altri dispositivi in suo possesso) al fine di consentire la tutela delle informazioni aziendali contenute nel dispositivo mobile;
- attenersi alle specifiche policy di sicurezza definite, impostando un codice di blocco (PIN) obbligatorio a tutela dell'accesso alle funzionalità del dispositivo mobile;
- utilizzare esclusivamente il client autorizzato per la gestione della/e cassetta/e di posta elettronica aziendale - installato e preconfigurato da ARCS;
- non cedere a terzi, a qualsiasi titolo, l'uso del telefono cellulare assegnato;
- non cedere a terzi, a qualsiasi titolo, l'uso dell'utenza telefonica assegnata;
- non attivare servizi interattivi con addebito sul conto telefonico a carico di ARCS.

Inoltre, ai sensi di quanto previsto dal gestore telefonico, i dipendenti sono tenuti a:

- non porre in essere atti e/o azioni che si risolvano, comunque, in una messa in pericolo o in un danno per l'operatività della rete;
- non utilizzare il servizio in modo da creare turbativa ad altri utenti;
- spegnere il telefono cellulare durante il rifornimento del carburante;
- spegnere il dispositivo quando si trovano in aereo, rispettando le disposizioni all'uopo impartite dalle autorità amministrative o dal comandante dell'aeromobile e, più in generale, adottare tutti gli accorgimenti per la sicurezza individuale e rispettare la normativa sull'uso dei telefoni cellulari nelle strutture sanitarie;
- non servirsi del telefono cellulare per effettuare comunicazioni che arrechino molestia o che violino le leggi vigenti.

Tutte le comunicazioni effettuate tramite l'utenza assegnata si presumono effettuate dal soggetto assegnatario, con ogni connessa responsabilità a suo carico, a partire dal momento dell'assegnazione.

9 ATTIVAZIONE/ASSEGNAZIONE UTENZA TELEFONICA

L'attivazione di una nuova utenza prevede il processo di "enrollment" (registrazione) del dispositivo nel sistema di gestione centralizzata MDM Airwatch attraverso l'installazione, a livello di sistema operativo -l'assegnatario non ha possibilità di rimuoverlo- del software Workspace ONE di VMware. A registrazione compiuta, al dispositivo verrà associato l'utilizzatore e saranno automaticamente installate e configurate tutte le applicazioni autorizzate.

10 SOSTITUZIONE DEL DISPOSITIVO MOBILE

L'assegnatario è tenuto a conservare in buono stato, ovvero in condizioni di normale usura, il telefono di servizio fornito in noleggio ad ARCS. Il contratto di noleggio dei dispositivi di telefonia mobile prevede il servizio di assistenza tecnica che garantisce la sostituzione in caso di:

- Guasto o malfunzionamento;
- Furto o smarrimento.

10.1 Guasti e malfunzionamenti

Per dare seguito alla sostituzione del dispositivo in caso di malfunzionamento, l'assegnatario può effettuare in maniera diretta e autonoma la chiamata verso il Customer Care 800.320.000 comunicando all'operatore le seguenti informazioni:

- numero di utenza;
- codice IMEI dell'apparato (riportato sul modulo di presa in carico);
- recapito telefonico;

- nome e cognome assegnatario;
- e-mail;
- difetto manifestato;
- Centro di Telefonia presso il quale ritirare il dispositivo sostitutivo.

Al termine della chiamata il Customer Care rilascia un codice che l'utente DEVE comunicare al centro TIM per il rilascio del nuovo apparato.

Come già descritto nella sezione "Attivazione/Assegnazione utenza telefonica", prima di essere utilizzato, l'eventuale nuovo apparato dovrà essere consegnato al GdT per l'enrollment all'interno della piattaforma MDM.

10.2 Furto e smarrimento

In caso di furto o smarrimento del dispositivo e/o della Carta SIM, l'assegnatario è tenuto a:

- sporgere formale denuncia presso le Autorità competenti avendo cura di far indicare nella denuncia il codice IMEI dell'apparato (visualizzabile sulla presa in carico);
- informare tempestivamente e senza ingiustificato ritardo il GdT all'indirizzo email tecnologie.informatiche@arcs.sanita.fvg.it l'avvenuto furto o smarrimento del telefono cellulare indicando le circostanze in cui è avvenuto e far pervenire allo stesso copia della denuncia per i conseguenti adempimenti (in assenza di denuncia, non potrà ad esempio essere attivata la procedura amministrativa prevista per l'eventuale sostituzione degli apparati forniti);

Il GdT, in seguito alla segnalazione pervenuta, procederà al blocco e/o alla sostituzione della scheda SIM e alla formattazione remota del dispositivo. Nel periodo intercorrente tra il furto/smarrimento della SIM e la sospensione della stessa, la responsabilità dell'eventuale utilizzo improprio resta a carico dell'assegnatario.

ARCS si riserva la 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.

11 CESSAZIONE/RESTITUZIONE/RIASSEGNAZIONE/RISCATTO

Al cessare delle condizioni che hanno condotto all'assegnazione dei dispositivi/SIM (cessazione del rapporto di lavoro, distacco presso altra amministrazione), non essendoci la necessità di avere strumenti lavorativi di supporto, la relativa utenza dovrà essere cessata o riassegnata.

Il Dirigente Responsabile della struttura assegnataria dovrà formalmente comunicare, entro 15 giorni e fermo restando che la responsabilità dell'utilizzo del dispositivo in tale periodo resta in carico al Dirigente Responsabile stesso, la summenzionata variazione al GdT.

Entro il medesimo termine, l'assegnatario è tenuto alla restituzione del dispositivo e della scheda SIM, nella propria confezione, integri e completi di tutti gli accessori ricevuti in dotazione; in difetto di ciò sarà carico del Dirigente Responsabile della struttura assegnataria il recupero e la restituzione dello stesso.

Anche nelle altre ipotesi in cui vengano meno i requisiti o le motivazioni che hanno dato luogo all'assegnazione (aspettativa o distacco di durata maggiore o uguale a sei mesi, compreso il caso di trasferimento dell'assegnatario presso diversa articolazione aziendale), sarà cura del Dirigente Responsabile avvisare il GdT e riconsegnare la strumentazione con le modalità in precedenza descritte. Qualora il Dirigente Responsabile della struttura assegnataria non restituisca il dispositivo/carta SIM secondo le tempistiche precedentemente riportate, ARCS si riserva la facoltà di richiedere gli eventuali danni da ciò derivanti.

Ancorché in costanza di sussistenza dei requisiti che hanno dato luogo all'assegnazione, il Dirigente Responsabile può, in ogni momento, disporre la revoca dell'autorizzazione e la conseguente riconsegna del dispositivo, il quale deve essere restituito integro, nella propria confezione e completo di tutti gli accessori ricevuti.

Il Dirigente Responsabile può provvedere in qualsiasi momento alla redistribuzione dei dispositivi/SIM all'interno della propria Struttura; tale redistribuzione dovrà essere tuttavia preventivamente comunicata ed autorizzata dal GdT.

A seguito dalla riassegnazione o della dismissione del dispositivo mobile, il GdT provvede alla redazione della necessaria modulistica (nuova presa in carico/dismissione del dispositivo ed aggiornamento della documentazione tecnico/amministrativa) ed alla cancellazione sicura (wipe) delle informazioni per proteggere le informazioni riservate e i dati personali secondo la normativa sulla privacy.

In concomitanza alla fine del rapporto lavorativo, l'assegnatario ha la possibilità di richiedere il riscatto della scheda SIM per il tramite del proprio Dirigente Responsabile; in tal caso il GdT si occuperà delle pratiche amministrative necessarie alla migrazione dell'utenza indicata da tipologia "Business" a "Consumer". Sarà poi cura dell'utente interfacciarsi con il Gestore Telefonico (ad esempio TIM, ...) per l'eventuale modifica della profilazione. È prevista la cessione della sola utenza; eventuali richieste di deroga sono da considerarsi eccezioni autorizzate dalla Direzione previa opportuna valutazione adeguatamente motivata del responsabile a cui riporta gerarchicamente la risorsa.

12 DISPONIBILITÀ

ARCS si riserva la facoltà di chiedere in restituzione, in ogni momento e senza preavviso, il dispositivo e la SIM assegnata in dotazione.

13 ATTIVAZIONE SERVIZI OPZIONALI

Per le sole utenze con dispositivo mobile ad uso esclusivo, sono predisposti i servizi "Dual Billing - Tim Tuo" e "Tim Tuo Roaming On Extra Spazio Economico Europeo" che possono essere fruiti dal dipendente con addebito a suo carico dei relativi costi.

L'assegnatario può, nei soli casi di assegnazione del dispositivo ad uso esclusivo, effettuare in maniera diretta e autonoma l'attivazione dei servizi mediante il Portale della Convenzione (<https://www.convenzione-telefoniamobile.it/mobile8>), previa registrazione e contestuale creazione delle Credenziali di autenticazione (UserID e Password).

Resta inteso che tutte le chiamate personali effettuate dall'utenza assegnata al dipendente si presumono da lui effettuate, con ogni conseguente responsabilità a suo carico.

13.1 Servizio "Dual Billing-Tim Tuo"

Il servizio "Dual Billing-Tim Tuo" consente all'assegnatario di fruire a titolo personale dei servizi offerti dall'operatore telefonico (es. TIM) alle medesime condizioni praticate all'ARCS e riportate nel documento *Corrispettivi e tariffe della Convenzione Telefonia Mobile 8*. La fruizione del servizio "Dual Billing-Tim Tuo" una volta attivato, è possibile mediante l'anteposizione del codice "4146" al numero chiamato o al destinatario dell'SMS.

ARCS non fornirà alcun tipo di servizio o assistenza riguardo problematiche che dovessero insorgere tra Gestore Telefonico e l'assegnatario del dispositivo per le quali è attivo l'apposito servizio di assistenza esterna.

Qualora il servizio fosse per qualsiasi motivo -anche temporaneamente- non attivo, al titolare del dispositivo è fatto divieto dell'utilizzo dello stesso per chiamate personali.

13.2 Servizio "Tim Tuo Roaming On Extra Spazio Economico Europeo"

L'opzione "Tim Tuo Roaming On Extra Spazio Economico Europeo" prevede che tutto il traffico originato e ricevuto in roaming in paesi fuori dallo Spazio Economico Europeo (fonia, SMS/MMS, dati e videochiamata) sia a carico del dipendente a prescindere dalla numerazione di origine o di destinazione e dell'utilizzo del codice "4146" ed è tariffato in base al listino previsto dalla Convenzione CONSIP attiva (al momento, Telefonia Mobile 8).

14 POLITICHE DI ACCESSO AI DATI ARCS

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 dati e dei sistemi, 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 mobili può avvenire solo sulla base delle indicazioni legate alla classificazione dei dati; di seguito quindi si identificheranno le seguenti tipologie di dispositivi:

- dispositivo mobile *gestito*: dispositivo sul quale è stato installato un software MDM fornito da ARCS;
- dispositivo mobile *verificato*: dispositivo verificato dal GdT su cui è stata configurata la posta elettronica tramite il protocollo ActiveSync, ma non un software MDM;
- dispositivo mobile *non gestito/verificato*: dispositivo non verificato dal GdT (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.

Tabella 1 – Accesso ai dati ARCS

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

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

- il canale di comunicazione deve essere crittografato (ad esempio tramite HTTPS);
- sul dispositivo verificato (a differenza del dispositivo gestito), non è permesso all'utente salvare "dati particolari" 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 in caso di utilizzo di *dispositivi mobili gestiti*, è facoltà di ARCS procedere alla formattazione del dispositivo da remoto nel caso venissero rilevate comprovate violazioni in termini di sicurezza (es. furto del dispositivo). Tale operazione resterà invece a carico dell'utente -attraverso l'apposita funzione disponibile su OWA- nel caso di *dispositivi mobili verificati*.

15 REGOLE PER LA GESTIONE E L'UTILIZZO DEI DISPOSITIVI GESTITI O VERIFICATI

L'uso dei dispositivi gestiti o verificati deve seguire le politiche e le seguenti regole di sicurezza stabilite da ARCS.

15.1 Software/Hardware

Non sono autorizzate modifiche hardware e/o software al dispositivo mobile (come, ad esempio, jailbreaking su iPhone oppure rooting su Android). Il sistema operativo ed i software installati sui dispositivi devono essere tenuti aggiornati.

Per i *dispositivi mobili gestiti*, gli aggiornamenti vengono controllati direttamente dalla piattaforma MDM e vengono inviati ai dispositivi mobili quando questi si trovano connessi ad una rete Wi-Fi. È quindi indispensabile che l'utente si colleghi periodicamente (almeno una volta a settimana) ad una rete Wi-Fi.

Per quanto riguarda invece i *dispositivi mobili verificati*, gli aggiornamenti sono a cura dell'utente e devono essere controllati settimanalmente ed applicati con una frequenza almeno mensile.

15.2 Accesso ai dispositivi mobili

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.

Qualora l'utilizzatore rinvenisse un accesso non autorizzato ai dati aziendali ARCS tramite il dispositivo mobile, dovrà immediatamente segnalarlo al GdT.

15.3 Applicazioni

L'utilizzatore potrà installare soltanto applicazioni provenienti dai repository ufficiali dei fornitori dei dispositivi mobili (es. Google Play, Apple iTunes), firmate digitalmente, nonché formalmente approvate dal GdT.

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 mobile personale verificato con all'interno la posta elettronica configurata tramite protocollo *ActiveSync*, il dipendente si atterrà alle disposizioni in materia di BYOD di cui al punto 15.7, in particolare al requisito **REQ-SIC-BYOD-02a**.

15.4 Reti telematiche

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.

15.5 Informazioni archiviate (per dispositivi verificati)

Gli utilizzatori non hanno il permesso di memorizzare le password in modo non cifrato sul proprio dispositivo. Inoltre, non sono autorizzati a copiare o inserire dati ARCS sul dispositivo mobile o sulla scheda di memoria rimovibile, a meno che i dati siano crittografati.

15.6 Regole comportamentali

Gli utilizzatori devono avvalersi di particolari accortezze nell'uso dei dispositivi mobili 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 mobili devono anche essere protetti fisicamente da furto, quindi, non devono essere lasciati dentro i veicoli, nelle stanze di hotel, ecc...

I dispositivi mobili, specialmente quelli contenenti "dati particolari", non devono mai essere lasciati incustoditi e, laddove possibile, devono essere tenuti in posti sicuri chiusi a chiave.

15.7 Bring Your Own Device (BYOD)

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 ARCS.

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, 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 Azienda 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 da ARCS e "gestiti".
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 dipendente deve adeguarsi alle disposizioni fissate nella presente policy
REQ-SIC-BYOD-02a	Nel caso in cui un 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 (Wi-Fi "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 alle reti ospiti, appunto perché non interconnesse a quelle aziendali, è permesso l'utilizzo di dispositivi personali

Codice	Comportamento applicato
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
REQ-SIC-BYOD-07	È d'obbligo l'osservanza da parte dei dipendenti, dei fornitori esterni e degli ospiti occasionali delle 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

16 TRATTAMENTO DEI DATI PERSONALI

L'adozione di tecnologie avanzate per garantire il corretto utilizzo del dispositivo e la sicurezza delle informazioni, avviene - insieme al trattamento effettuato per finalità amministrative - nel rispetto del principio di pertinenza e non eccedenza, senza l'utilizzo di strumentazioni mirate al controllo dell'utente e in conformità all'informativa diffusa ai dipendenti ai sensi dell'art. 13 del Regolamento 2016/679/UE, cui si fa integrale rinvio.

I dati sono resi accessibili ai soggetti autorizzati al loro trattamento nelle modalità descritte nel presente documento; possono essere inoltre resi accessibili o comunicati ad Organismi di vigilanza, Autorità giudiziarie nonché a tutti gli altri soggetti ai quali la comunicazione sia obbligatoria per legge o per l'espletamento delle finalità per cui i dati sono raccolti.

17 DISPOSIZIONI FINALI, ENTRATA IN VIGORE E PUBBLICITÀ

La presente policy, proposta dal Responsabile della struttura Tecnologie Informatiche, entra in vigore dalla data di esecutività del relativo Decreto di adozione.

Con l'entrata in vigore della stessa, tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti. Per quanto non espressamente previsto sarà fatto riferimento alla normativa vigente in materia.

La presente Policy verrà debitamente e tempestivamente portata a conoscenza di tutti i dipendenti ARCS.

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 ARCS.

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

18 NOTIFICHE DI NON-CONFORMITÀ, MISURE DISCIPLINARI E AGGIORNAMENTI ALLA POLITICA

Dipendenti, collaboratori e soggetti terzi equiparabili a Personale interno sono tenuti a rispettare la presente policy.

Il mancato rispetto o la violazione delle regole contenute in questa policy, qualora siano ravvisabili profili quantomeno colposi nella condotta osservata, è perseguibile mediante l'attivazione di procedimenti disciplinari previsti dalla vigente normativa.

Il GdT valuterà qualsiasi eccezione dall'osservanza di particolari disposizioni contenute nella presente policy. 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.

19 TERMINOLOGIA E ABBREVIAZIONI

Termine	Definizione
ARCS	Azienda Regionale di Coordinamento per la Salute
Assegnatario	Ogni soggetto (dipendente e collaboratore) cui è stato concesso l'utilizzo di telefoni cellulari di servizio e/o di strumenti per la connettività dati da rete mobile. Per i dispositivi ad uso "struttura", la responsabilità è in capo al Dirigente Responsabile della Struttura richiedente.
BYOD	L'approccio Bring Your Own Device (BYOD) è l'insieme di criteri in un'azienda che consente ai dipendenti di utilizzare i propri dispositivi (telefono, laptop, tablet o altro) per accedere alle applicazioni e ai dati aziendali
Centro di Telefonia	Con l'adesione alla convenzione Consip Telefonia Mobile 8, si intende il Centro TIM al quale fare riferimento per l'assistenza. Alla data di redazione della presente policy, a Udine sono presenti: "Centro Tim Piazzale Gabriele D'Annunzio, 19" e "Centro TIM Parco Commerciale Terminal Nord"
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

Dati particolari	Art. 9 UE 679/2016. "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."
Dirigente Responsabile	Responsabile della struttura. Soggetto preposto alle richieste di nuovi dispositivi di telefonia mobile e/o richieste di modifica alla configurazione degli stessi
Disponibilità	Requisito di sicurezza in base al quale un'informazione deve essere accessibile e utilizzabile su richiesta dai soggetti autorizzati.
GdT (Gestore della telefonia) Aziendale	La struttura operativa preposta alla gestione della telefonia mobile (SSD Tecnologie Informatiche)
Gestore telefonico	Aggiudicatario della Convenzione Consip Attiva (al momento della redazione della presente Policy, TIM)
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)
Information Commissioner's Office	la prima Autorità europea per la protezione dei dati personali ad aver emanato delle linee guida correlate all'utilizzo del BYOD (Bring Your Own Device)
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
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	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 (BYOD) che consentono ai dipendenti di accedere ai dati aziendali, ai file e alle applicazioni sui propri dispositivi personali.
Misure minime di sicurezza ICT per le	Le misure minime di sicurezza ICT emanate dall'AgID allo scopo di contrastare le minacce informatiche più frequenti della pubblica amministrazione italiana;

pubbliche amministrazioni	consistono in controlli di natura tecnologica, organizzativa e procedurale, con tre livelli di attuazione
Personale dipendente	Per personale dipendente, ai fini della presente procedura, si intende: - personale assunto alle dipendenze dell'Azienda con contratto di lavoro a tempo indeterminato o determinato; - personale dipendente di altri enti comandato a prestare servizio presso l'Azienda; - personale in servizio presso l'Azienda mediante somministrazione di lavoro interinale
Password	componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica
Policy	documento che riporta obiettivi ed indirizzi generali, relativi alle principali funzioni ed attività assistenziali e gestionali
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.
SIM CARD	acronimo di Subscriber Identity Module (SIM). Rappresenta la scheda rimovibile per i telefoni cellulari. Allo stato dell'arte vengono prodotte in 3 formati (mini, micro e nano) da scegliere funzionalmente al dispositivo a cui verranno associate.
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 programmi, oppure da uno o più dati, oppure da una combinazione delle due
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." – Tecnologie Informatiche
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

Traffico dati	il traffico per la trasmissione dati dal terminale mobile verso gli APN (Access Point Node)
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
Utente	ciascuna persona che accede alle risorse informatiche aziendali
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)
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.
Wi-Fi	Wi-Fi è una tecnologia che consente agli utenti finali e dispositivi mobili di collegarsi tra loro attraverso una rete locale senza fili (WLAN)
Wipe	cancellazione sicura dei dati

20 ALLEGATI

Al presente documento viene allegata la seguente documentazione:

- Allegato 1 – “Nuova richiesta dispositivo mobile o variazione configurazione”
- Allegato 2 – “Presa in carico dispositivo telefonico aziendale”
- Allegato 3 – “Delega per presa in carico dispositivo telefonico aziendale”
- Allegato 4 – “Registro assegnazioni dispositivi”

Alla c.a.
Del Responsabile della
SSD Tecnologie Informatiche

Trasmesso mezzo GIFRA all'indirizzo:
tecnologie.informatiche@arcs.sanita.fvg.it

RICHIESTA DISPOSITIVO TELEFONICO MOBILE

Il/La sottoscritto/a **NOME e COGNOME RESPONSABILE di STRUTTURA**, nella sua veste di Responsabile e Referente interno della struttura **NOME STRUTTURA**, verificata la necessità di attivare un nuovo dispositivo telefonico mobile per il pieno adempimento dei compiti assegnati

CHIEDE L'ATTIVAZIONE

di:

- ☐ SIM Telefonica.
☐ Telefono aziendale.

I dispositivi richiesti sono destinati a:

- ☐ dipendente ARCS:
Nome e Cognome **NOME E COGNOME**
Codice Fiscale **XXXXXX00X00X000X**

per: ¹

- ☐ Adempimenti necessari per attuare obblighi di pubblico interesse;
☐ Utenze ad uso allarmistica;
☐ Utenze ad uso struttura;
☐ Utenze afferenti alla segreteria di direzione preventivante individuate dalla direzione strategica;
☐ Responsabili di struttura semplice (SS), semplice dipartimentale (SSD) e complessa (SC).

 *In caso di dispositivo ad uso struttura esiste l'obbligo di redigere ed aggiornare un "registro assegnazioni"*

Lo/a scrivente, si impegna altresì a comunicare tempestivamente qualunque variazione dello stato di servizio del soggetto da autorizzare nel momento stesso in cui vengano meno le condizioni per poter utilizzare i dispositivi richiesti.

Motivo della richiesta _____

Udine _____

Il Dirigente Responsabile
firmato digitalmente

¹Rif. Policy Telefonia Mobile § 3

PRESA IN CARICO DISPOSITIVO TELEFONICO AZIENDALE

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

CONCEDE IN USO E CONSEGNA

Al/alla Sig./Sig.ra **NOME COGNOME**, incardinato/a presso la struttura **STRUTTURA** i seguenti dispositivi:

Dati identificativi dell' apparecchio telefonico consegnato
Marca e modello apparato:
Serial Number (IMEI)***:

Dati identificativi della scheda SIM consegnata
Numero Telefonico:
PIN:
PUK:
Numero SIM (ICCID)****:

Accessori:

Dati identificativi dell' apparecchio telefonico restituito
Marca e modello apparato:
Serial Number (IMEI)***:

Gli asset aziendali sono consegnati alle seguenti condizioni:

- a) i beni sopra descritti debbono servire per adempiere alle mansioni lavorative assegnate;
- b) l'utente si obbliga come previsto dal Codice Penale e dal "Codice Etico di ARCS":
 - a conservare e a custodire i beni in oggetto con la massima cura e diligenza;
 - a non destinare i beni in oggetto ad altri usi che non siano quelli sopra previsti inerenti l'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);
- c) 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;

- 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) 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;
- f) 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;
- g) ARCS si riserva altresì la facoltà di chiedere il risarcimento in caso di danno causato al bene intenzionalmente e/o per colpa dell'utente.
- h) Il dispositivo viene pre-configurato da ARCS TI (*enrollment*) ed inserito in un contesto MDM (Mobile Device Management) fornito da TIM in modalità SaaS (Software as a Service - WEB).

Letto, approvato e sottoscritto

Udine, il

Firma dell'assegnatario

I dati raccolti tramite il presente modulo verranno trattati unicamente per le finalità ivi indicate e nel rispetto dei principi di liceità e correttezza ai sensi del Reg. UE 679/2016 e del Codice Privacy s.m.i.

Per ulteriori informazioni sul trattamento dei dati personali connessi all'utilizzo dei dispositivi è possibile consultare l'informativa privacy estesa reperibile in  S: → Bacheca Lettura → Tecnologie Informatiche → Telefonia

RICONSEGNA

Con la presente, l'incaricato della struttura Tecnologie Informatiche, riceve dal/dalla

Sig/ra.: _____

il materiale sopra individuato in stato funzionante e con i normali segni di usura dovuti all'uso.

Udine, il

Nome e Cognome Incaricato T.I.

Firma incaricato T.I.

Alla c.a.
Del Responsabile della
SSD Tecnologie Informatiche

PRESA IN CARICO DISPOSITIVO TELEFONICO AZIENDALE

Il/La sottoscritto/a
nato/a a il
residente in via C.A.P.
Città
Documento di Identità n° rilasciato da il

DELEGA

Il/La Sig/Sig.ra
a ritirare per proprio conto il dispositivo telefonico mobile aziendale assegnatomi.

Con la sottoscrizione del presente modulo, il delegante dichiara che ha preventivamente preso visione di quanto riportato nel Regolamento per ***"l'assegnazione e utilizzo dei dispositivi di telefonia mobile di servizio"***

Firma leggibile



Allegare alla presente fotocopia del documento di identità del delegante
Il delegato si presenti con documento d'identità in corso di validità

REGISTRO ASSEGNAZIONE APPARECCHI CELLULARI				Codice identificazione file: Rev.01 Ed.01	
PER DISPOSITIVI DI STRUTTURA		ANNO		Pagina	di

Utenza (num. telefono)	Nome Cognome assegnatario	Motivazione Esigenze Servizio	Data consegna	Ora consegna	Data restituzione	Ora restituzione