PORTS of GENOA
VADO LIGURE ▪ SAVONA
PRA' ▪ GENOVA

AUTORITÀ DI SISTEMA PORTUALE DEL MAR LIGURE OCCIDENTALE

Decreto N. 1102

IL PRESIDENTE

VISTA la legge 28 gennaio 1994, n. 84, di riordino della legislazione in materia portuale e successive modificazioni e integrazioni ed in particolare il Decreto Legislativo 4 agosto 2016, n. 169 e il Decreto Legislativo 232 del 13 dicembre 2017;

VISTO il decreto del Ministro delle Infrastrutture e dei Trasporti del 1° dicembre 2016 n. 414, notificato in data 2 dicembre 2016, di nomina del Dott. Paolo Emilio Signorini nella carica di Presidente dell'Autorità di Sistema Portuale del Mar Ligure Occidentale;

VISTA la deliberazione assunta dal Comitato di Gestione nella seduta dell'8 maggio 2017, prot. n. 31/10/2017, concernente la nomina del Dott. Marco Sanguineri a Segretario Generale dell'Autorità di Sistema Portuale del Mar Ligure Occidentale a far data dal 15 maggio 2017, nonché il decreto n. 606 del 9 maggio 2017 con il quale si rende esecutiva tale nomina;

VISTO il Regolamento di Amministrazione e di Contabilità dell'ex Autorità portuale approvato dal Comitato Portuale nella seduta del 23 aprile 2007, integrato dal Ministero dei Trasporti e dal Ministero dell'Economia e delle Finanze con nota del 26 giugno 2007, integrato dal Comitato Portuale con delibera 117/2 nella seduta del 29 novembre 2011 ed approvato dal Ministero delle Infrastrutture e dei Trasporti, di concerto con il Ministero dell'Economia e delle Finanze, con nota M_TRA/PORTI/3927 del 26 marzo 2012;

VISTO l'art. 22 comma 4 del Decreto Legislativo 4 agosto 2016, n. 169 con cui, fino all'approvazione del regolamento di contabilità di cui all'art. 6, comma 9, della Legge n.84 del 1994, come modificato dal decreto di cui trattasi, l'Autorità di Sistema Portuale applica il regolamento di contabilità della soppressa Autorità portuale dove ha sede la stessa Autorità di Sistema Portuale;

VISTO l'art. 8 della Legge 84/94 ed in particolare il comma 2 che dispone che al Presidente spetta la gestione delle risorse finanziarie in attuazione del piano di cui all'articolo 9, comma 5, lettera b);

VISTA la deliberazione assunta dal Comitato di Gestione nella seduta del 4 luglio 2017, prot. n. 45/6, con la quale è stata adottata la nuova dotazione organica dell'AdSP, approvata dal Ministero delle Infrastrutture e dei Trasporti con nota prot. n. 21803 del 31 luglio 2017;

VISTO il decreto n. 1889 del 21 novembre 2017, con il quale è stata approvata la nuova organizzazione, la declaratoria delle strutture dirigenziali e il relativo funzionigramma dell'AdSP, nonché il decreto n. 2077 del 14 dicembre 2017 che posticipa al 1° gennaio 2018 l'efficacia di tale decreto;

VISTI i decreti n. 2306 del 29 dicembre 2017 e n. 1129 del 15 giugno 2018 di attribuzione degli incarichi dirigenziali alle strutture dell'AdSP di cui al decreto n. 1889 del 21 novembre 2017;

VISTO il bilancio di previsione 2019 approvato dal Comitato di Gestione con Delibera n. 85/4/2018 nella seduta del 07.12.2018 ed approvato dal Ministero delle Infrastrutture e dei Trasporti con nota prot. n. 6321 del 4.3.2019 (prot. AdSP n. 5841 del 04.03.2019);

VISTE le prime note di variazione al Bilancio di Previsione 2019 approvate dal Comitato di Gestione con Delibera n. 46/6/2019 del 27/6/2019 comprendenti altresì l'aggiornamento del Programma triennale delle opere infrastrutturali 2019-2021 e l'elenco degli interventi della programmazione 2019-2021 di cui al Programma ex Art. 9 Bis L.130/2018;

VISTE le Circolari AgID, Agenzia per l'Italia Digitale, n. 179/2016 e n. 2/2017 del 18 aprile 2017 riguardanti la transizione alla modalità operativa digitale e l'implementazione delle misure minime di sicurezza ICT per le Pubbliche Amministrazioni;

VISTA la Legge del 7 agosto 2015 n.124 "Carta della Cittadinanza Digitale", in materia di riorganizzazione delle amministrazioni pubbliche;

VISTO il Piano Triennale di Prevenzione della Corruzione dell'AdSP 2018-2020 (PTPC), approvato con delibera del Comitato di Gestione dell'AdSP n. 1/1/2018 in data 31/1/2018,

VISTA la Direttiva (UE) 2016/1148 e suoi adeguamenti e integrazioni (NIS);

VISTO il Decreto Legislativo che recepisce e attua la direttiva (UE) 2016/1148 del Parlamento Europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi dell'Unione, che qui si intende integralmente riportato (NIS), al fine di assicurare la qualità dei servizi, la prevenzione dei fenomeni di corruzione, il rispetto dei doveri costituzionali di diligenza, lealtà, imparzialità e servizio esclusivo alla cura dell'interesse pubblico, e la salvaguardia del patrimonio fisico, logico / informatico e organizzativo dell'AdSP;.

VISTI il Regolamento (UE) 2016/679 e suoi adeguamenti e integrazioni (GDPR), il D.Lgs. 30 giugno 2003, n. 196 e successive modifiche ed integrazioni, nonché i diversi provvedimenti del Garante in materia di protezione dei dati personali.

PREMESSO che l'Autorità di Sistema Portuale del Mar Ligure Occidentale è dotato di apparati di telefonia mobile e SIM utilizzate dal personale dell'Ente;

PREMESSO che l'assegnazione e l'uso di sistemi telefonici mobili deve rispondere all'interesse ed alle esigenze dell'Amministrazione, al miglioramento della qualità del lavoro, consentendo il soddisfacimento di bisogni lavorativi in un quadro di economicità ed efficienza;

RAVVISATA, quindi, la necessità di regolamentare l'assegnazione e l'uso delle apparecchiature di telefonia mobile, adottando apposito Regolamento;

SENTITI il Responsabile della Protezione dei Dati, il Dirigente del Servizio Sistemi Informativi, Telematica e Sistema di Gestione nonché Responsabile per la Transizione al Digitale ed il Segretario Generale,

DECRETA

1. è approvato il Regolamento "*Utilizzo degli Strumenti Informatici Aziendali - Telefoni Cellulari*" allegato al presente decreto a farne parte integrante e sostanziale;

2. il Regolamento entra immediatamente in vigore ed abroga eventuali precedenti Regolamenti incompatibili con esso;

3. di pubblicare il Regolamento di cui trattassi in via permanente sul sito *intranet* dell'Autorità di Sistema Portuale del Mar Ligure Occidentale e sul sito Amministrazione Trasparente dell'Ente.

IL PRESIDENTE
Dott. Paolo Emilio Signorini

Genova, li 29-07-2019

decreto delega 1085
del 25-07-2019

REGOLAMENTO

UTILIZZO DEGLI STRUMENTI INFORMATICI AZIENDALI

TELEFONI CELLULARI

INDICE

1. SCOPO DEL REGOLAMENTO

Il corretto utilizzo dei Telefoni Cellulari aziendali (compresi nella definizione "Strumenti Informatici Aziendali", utilizzata successivamente) risponde contestualmente alle esigenze dell'Autorità di Sistema Portuale del Mar Ligure Occidentale (di seguito AdSP) ed alle necessità legate al lavoro di dipendenti/collaboratori autorizzati al loro utilizzo (in seguito indicati come "Persone Autorizzate").

Il presente Regolamento ha, quindi, lo scopo di definire le modalità e i doveri che ogni Persona Autorizzata deve osservare nell'utilizzo dei Telefoni Cellulari che l'AdSP mette a sua disposizione, nonché di illustrare gli interventi e le verifiche che l'AdSP può effettuare, nel rispetto della normativa vigente, al fine di tutelare le proprie risorse.

2. RESPONSABILITÀ

Tutti gli Strumenti Informatici Aziendali, nonché la Rete Aziendale, devono essere utilizzati e gestiti dalla singola Persona Autorizzata nel rispetto dei principi di diligenza e correttezza, in modo conforme al presente Regolamento.

L'AdSP si riserva di verificare, nel rispetto della tutela dei Dati Personali e del diritto alla riservatezza di ogni Persona Autorizzata e, più in generale, nel rispetto di quanto previsto dalla vigente normativa anche in materia di controllo a distanza dei lavoratori, che l'utilizzo degli Strumenti Informatici Aziendali avvenga in maniera conforme al presente Regolamento e che, in particolare, non venga scaricato/installato/utilizzato alcun software non autorizzato o che, comunque, possa compromettere gli Strumenti Informatici Aziendali, la Rete Aziendale o i dati Aziendali .

3. FINALITÀ

L'AdSP ritiene fondamentale la comprensione, il rispetto e la corretta applicazione di quanto indicato nel presente Regolamento, al fine di arginare il più possibile i rischi connessi ad un eventuale utilizzo non corretto delle proprie risorse informatiche, proteggendo le Persone Autorizzate da azioni illegali e/o pericolose e contestualmente salvaguardando il patrimonio dei dati dell'AdSP.

L'utilizzo degli Strumenti Informatici Aziendali da parte della Persone Autorizzate, pertanto, deve sempre ispirarsi ai principi di massima diligenza, buona fede e correttezza, a tutela tanto degli interessi dell'Ente di appartenenza quanto della posizione delle stesse Persone Autorizzate.

Si ricorda come un uso improprio e/o non conforme ai suddetti principi degli Strumenti Informatici Aziendali ovvero della Rete Aziendale, della posta elettronica, del *file sharing* (file condivisi sulla Rete Aziendale) e di Internet potrebbe esporre l'AdSP a serie conseguenze pregiudizievoli, quali, a titolo meramente esemplificativo e non esaustivo, accessi non autorizzati – anche attraverso l'introduzione di *virus*, ma più in generale *malware* - al suo sistema informatico o al suo patrimonio di dati e notizie, o, ancora, furti o divulgazioni di informazioni segrete, confidenziali e/o riservate, sottrazione e/o trattamenti illeciti di dati personali.

In ragione pertanto di primarie esigenze organizzative, produttive e di sicurezza, l'AdSP ha adottato il presente Regolamento, che fornisce precise indicazioni alle Persone Autorizzate circa le modalità di funzionamento della Posta Elettronica Aziendale, dell'accesso a Internet, in linea a quanto previsto per tutti gli Strumenti Informatici Aziendali e della Rete Aziendale;

- codifica regole di comportamento da rispettare nell'uso di detti strumenti, onde evitare problemi, disservizi e maggiori costi (di manutenzione o di altro tipo) ovvero minacce alla Rete Aziendale o alla sicurezza dei sistemi e dei dati in essi contenuti;
- istituisce strumenti che, nel rispetto delle previsioni di cui agli artt. 4 e 8 della Legge 20 maggio 1970 n. 300 ("Statuto Lavoratori") e successive modificazioni, nonché dei principi di correttezza,

pertinenza e non eccedenza di cui all'art. 5 del 2016/679 (GDPR), consentano di evitare e prevenire condotte improprie nell'utilizzo degli Strumenti Informatici Aziendali, allo scopo di salvaguardare le informazioni aziendali, gli standard qualitativi dei servizi erogati sia internamente che resi al Pubblico, e specificatamente le conoscenze dell'AdSP.

L'AdSP garantisce che con il presente Regolamento:

- non si intende adottare e/o autorizzare e/o istituire, in alcun modo, sistemi e/o strumenti di controllo a distanza e/o in forma occulta delle opinioni, abitudini e/o dell'attività dei dipendenti o collaboratori della medesima o comunque di quanti legittimamente utilizzino, su autorizzazione dell'AdSP, gli Strumenti Informatici e la Rete Aziendale, che rimangono vietati e non consentiti;
- s'intende unicamente, istituire forme di verifica del corretto uso degli Strumenti Informatici Aziendali, esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro, per la tutela del patrimonio aziendale e della sicurezza del sistema e della Rete Aziendale dell'AdSP, al fine di tutelare quest'ultima da eventuali danni che possano essere generati e che siano riconducibili ad una condotta posta in essere dalla Persona Autorizzata in violazione del presente Regolamento e/o in violazione di norme di legge, inadempimenti contrattuali e/o dalla commissione di fatti illeciti e/o aventi rilevanza penale e/o disciplinare.

4. RIFERIMENTI NORMATIVI

Di seguito si riporta l'impianto normativo di riferimento del presente Regolamento.

- Circolare AgID, Agenzia per l'Italia Digitale, n. 179/2016 e n. 2/2017 del 18 aprile 2017 riguardante la transizione alla modalità operativa digitale e l'implementazione delle misure minime di sicurezza ICT per le Pubbliche Amministrazioni.
- Legge del 7 agosto 2015 n.124 ''Carta della Cittadinanza Digitale'', in materia di riorganizzazione delle amministrazioni pubbliche.
- Piano Triennale di Prevenzione della Corruzione dell'AdSP 2018-2020 (PTPC), approvato con delibera del Comitato di Gestione dell'AdSP n. 1/1/2018 in data 31/1/2018, e che comprende un sistema organico di azioni e misure specificamente concepite a presidio del rischio corruttivo, in attuazione degli strumenti normativi di seguito elencati e a tutela della trasparenza ed integrità all'interno della struttura dell'AdSP profondamente rinnovata a seguito del DLgs 169/2016.
  - Legge 6 novembre 2012, n. 190, recante "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione".
  - DLgs n. 33/2013 concernente "Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni".
  - DPR n.62/2013 "Regolamento recante codice di Comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165".
  - Decreto Legislativo n.39 dell'8 aprile 2013, "Disposizioni in materia di inconferibilità ed incompatibilità di incarichi presso le pubbliche amministrazioni e presso gli enti privati in controllo pubblico, a norma dell'art.1, co. 49 e 50 della legge 6 novembre 2012, n.190".
  - Decreto Legislativo n. 97 del 25 maggio 2016, concernente "Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione, pubblicità e trasparenza".
  - Legge 30 novembre 2017 n. 179 (G.U.R.I. n. 291 del 14 dicembre 2017) concernente le "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato".
- Direttiva (UE) 2016/679 e suoi adeguamenti e integrazioni (GDPR).
  - Decreto legislativo del 18 maggio 2018, n. 51, che adegua il Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196) alle disposizioni del

Regolamento (UE) 2016/679 – GDPR.

- Decreto n.101/18 del 10 agosto 2018, entrato ufficialmente in vigore dal 19 settembre 2018, che qui si intende integralmente riportato, che adegua il Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196) alle disposizioni del Regolamento (UE) 2016/679 – GDPR.

- Direttiva (UE) 2016/1148 e suoi adeguamenti e integrazioni (NIS).
  - Decreto Legislativo che recepisce e attua la direttiva (UE) 2016/1148 del Parlamento Europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi dell'Unione, che qui si intende integralmente riportato (NIS), al fine di assicurare la qualità dei servizi, la prevenzione dei fenomeni di corruzione, il rispetto dei doveri costituzionali di diligenza, lealtà, imparzialità e servizio esclusivo alla cura dell'interesse pubblico, e la salvaguardia del patrimonio fisico, logico / informatico e organizzativo dell'AdSP secondo le normative vigenti alla data e sopra riportate.
- Provvedimenti del Garante in materia di protezione dei dati personali.

5. DEFINIZIONI

- **Gestore del Sistema**: figura professionale che si occupa di gestire e manutenere la rete informatica, gli apparati e i sistemi di sicurezza e i database nonché di ogni altro sistema tecnico legato alla gestione degli strumenti informatici.
- **Dato Personale**: 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;
- **Persona Autorizzata**: dipendente/collaboratore autorizzato all'utilizzo degli Strumenti Aziendali.
- **Posta Elettronica Aziendale**: strumento che permette alla Persona Autorizzata di disporre di un account di posta elettronica sul dominio aziendale @portsofgenoa.com.
- **Rete Aziendale**: rappresenta il perimetro digitale dell'AdSP, contenente anche Dati Personali e/o informazioni riservate, comprensivo dei dispositivi hardware/software sia per la gestione dei servizi interni (es. switch, LAN, Wi-Fi) che dei collegamenti da o verso l'esterno (es. VPN);
- **Strumenti Informatici Aziendali**: l'insieme di Device Fissi e Device Mobili, compresi i Telefoni Cellulari le SIM CARD ad essi associate, e assegnati dall'AdSP alle Persone Autorizzate al fine di svolgere le proprie mansioni;

6. MODALITÀ OPERATIVE

6.1 Utilizzo dei telefoni cellulari

6.1.1 Regole generali

I telefoni cellulari e le relative SIM CARD vengono assegnati alle Persone Autorizzate su richiesta del Direttore/Dirigente di riferimento. La richiesta e la consegna del terminale e della SIM sono formalizzate attraverso moduli di sistema in vigore.

I telefoni cellulari e le SIM CARD, in ragione della loro portabilità, devono essere gestiti dalla Persona Autorizzata, che ne diventa custode, con particolare cura e diligenza, adottando tutti i ragionevoli accorgimenti per evitare eventuali danni e/o sottrazioni, sia durante gli spostamenti sia durante l'utilizzo nei locali dell'Ente.

Specificamente, si ricorda che i telefoni cellulari:

- non possono essere oggetto di impostazioni applicate dalla Persona Autorizzata tali da inficiare in alcun modo i livelli di sicurezza previsti dalle politiche di sicurezza dell'AdSP;
- possono essere facilmente rubati o smarriti e, quindi, comportare la perdita, oltre che dello strumento in sé, di informazioni importanti per l'AdSP, ivi compresi Dati Personali; pertanto la Persona Autorizzata dovrà tutelare le informazioni aziendali presenti sul Device Mobile mediante un PIN di sblocco della SIM, da inserire al momento della riaccensione e un sistema di blocco (PIN Utente o Fingerprint) quando se ne interrompe l'uso, in modo che soggetti non autorizzati non abbiano accesso ai dati in esso contenuti;
- ribadendo quanto sopra, al fine di evitare accessi indebiti, non è consentito eliminare o bypassare l'utilizzo di un codice di sicurezza inserito su ogni apparato (PIN Utente), oltre al PIN di sblocco della SIM, che non può dunque essere rimosso; il PIN non deve essere comunicato a terzi e deve essere custodito con la massima diligenza;
- eventuali guasti e/o la messa fuori uso di quanto consegnato devono essere tempestivamente comunicati dalla Persona Autorizzata all'ufficio Informatica e Sviluppo ICT.

Anche al fine di evitare di compromettere la disponibilità e la sicurezza di Sistemi e di Strumenti Informatici Aziendali nonché di evitare responsabilità nei confronti di terzi, **è espressamente vietato**:

- utilizzare la SIM Card su un dispositivo diverso da quello di servizio;
- concedere in uso il Device Mobile a soggetti terzi;
- installare ed utilizzare programmi e/o APP non espressamente autorizzati dall'AdSP;
- la conservazione e la trasmissione di programmi, APP, file, contenuti multimediali ed altro in violazione delle rispettive licenze di utilizzo (in proposito, si vedano gli obblighi imposti dalla L. 22 aprile 1941, n. 633 e ss. mm. ii. sulla protezione del diritto d'autore e altri diritti connessi al suo esercizio);
- ascoltare e/o visionare e/o scaricare programmi, film, file audio/musicali sugli Strumenti Informatici Aziendali, che non siano correlati alle attività lavorative;
- effettuare configurazioni o modifiche atte ad utilizzare l'apparato in dotazione come strumento di comunicazione con fini terzi rispetto a quelli consentiti nel presente documento, quali, a mero titolo esemplificativo, impostare l'utilizzo come access point per dispositivi terzi che non siano Strumenti Informatici Aziendali;
- fare copia, in qualunque forma e su qualunque tipo di supporto fisico o elettronico, di Dati Personali e/o informazioni riservate e/o file dell'AdSP nella disponibilità della Persona Autorizzata al fine di farne un uso personale o per trasferirli a terzi;
- utilizzare programmi informatici o strumenti per intercettare, falsificare, alterare o cancellare per finalità illecite il contenuto di comunicazioni e/o documenti informatici;
- modificare le configurazioni aziendali impostate sul telefono aziendale, salvo autorizzazione preventiva dell'Ufficio Informatica e Sviluppo ICT;
- collocare, anche temporaneamente, sugli Strumenti Informatici Aziendali o nella Rete Aziendale qualsiasi file che non sia attinente allo svolgimento dell'attività lavorativa.

Salvo quanto precede, la Persona Autorizzata si impegna comunque a prendere ogni accorgimento di sicurezza idoneo per la salvaguardia delle informazioni aziendali.

Si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software e su tutte le opere di ingegno (es: film, file musicali, ecc.), che impone la presenza nel sistema di software regolarmente licenziati o comunque liberi e quindi non protetti dal diritto d'autore, vengono sanzionate anche penalmente.

Sul punto, l'AdSP utilizza sistemi in grado di impedire l'accesso a siti non pertinenti con l'attività lavorativa o che offrono contenuti palesemente violativi del diritto d'autore.

Ogni eccezione a quanto riportato sopra deve essere approvata per iscritto dall'Ufficio Informatica e Sviluppo ICT.

6.1.2 Gestione anomalie

La Persona Autorizzata che rilevi attività anomale da parte del telefono cellulare che ha in dotazione è tenuta ad informare prontamente l'Ufficio Informatica e Sviluppo ICT.

Nel caso in cui il sistema di gestione degli apparati (vedi paragrafo gestione cellulari – MDM 6.1.4), anche indipendentemente dalle segnalazione della Persona Autorizzata, allerti su ripetute attività anomale da parte del telefono cellulare (es. traffico anomalo, presenza di virus, attività comunque in grado di causare danno alla normale operatività aziendale o a soggetti terzi, furto o smarrimento), l'AdSP si riserva di intervenire prontamente, segnalando il problema al Dirigente/Direttore di riferimento al fine di individuarne le cause ed adottare le azioni correttive necessarie alla sua risoluzione, incluso l'eventuale blocco del dispositivo.

I telefoni possono essere revocati/disabilitati dall'AdSP in caso di uso improprio, decadenza dei presupposti di conferimento e/o in ogni altro caso ritenuto opportuno, ad esempio per furto o smarrimento dello strumento.

6.1.3 Protezione delle informazioni aziendali

La Persona Autorizzata deve attuare quanto necessario ad evitare la perdita di informazioni aziendali rilevanti contenute nella memoria dei dispositivi mobili, ad esempio a seguito di guasto, smarrimento/furto. A tal fine, ove possibile, è suggerito alla Persona Autorizzata di scaricare quanto prima possibile i file di lavoro (immagini/testi) ovvero di concordare appropriate procedure di backup con l'Ufficio Informatica e Sviluppo ICT.

6.1.4 Gestione cellulari – MDM (Mobile Device Management)

L'AdSP utilizza un sistema (MDM) preposto alla configurazione centralizzata degli apparati tecnicamente necessario alla loro gestione standardizzata. Il ruolo generale di un MDM consiste nell'aumentare la sicurezza e le funzionalità aziendali, pur garantendo flessibilità per la Persona Autorizzata.

Alcune delle funzioni principali del sistema di gestione MDM sono:

- la corretta configurazione dell'apparato per un insieme di applicazioni, funzioni o procedure aziendali;
- l'aggiornamento delle apparecchiature, applicazioni, funzioni o politiche in modo scalabile;
- l'utilizzo delle applicazioni installate;
- la diagnostica da remoto utile nei casi di smarrimento / furto / malfunzionamento.

La finalità dell'installazione del sistema MDM è di standardizzare le funzioni di supporto e di ridurre eventuali rischi aziendali, ottimizzando la funzionalità e la sicurezza della rete di comunicazioni mobili di AdSP.

Sull'apparato consegnato è stato preinstallato un "agent", che non deve essere modificato, finalizzato a consentire, sia al dipendente che all'Amministrazione, una gestione il più possibile efficace e sicura del dispositivo.

In nessun caso i sistemi ed i software preinstallati saranno utilizzati dall'Ente come programmi di controllo dell'attività del dipendente e non saranno effettuati controlli indiscriminati.

Tenuto conto che l'utente può abilitare e/o disabilitare la funzione di geolocalizzazione-GPS, si precisa che, in ogni caso, il GPS non raccoglie i dati e l'Ente non procederà alla raccolta dei dati relativi al sistema di geolocalizzazione

In ogni caso, eventuali informazioni riferibili ai possessori dei dispositivi saranno utilizzate per finalità esclusivamente tecniche, dunque non riconducibili a quelle di controllo degli stessi.

6.1.5 Misure specifiche

Si elencano di seguito le misure specifiche adottate dall'AdSP e che la Persona Autorizzata è tenuta a non modificare e, ove possibile, segnalarne l'eventuale anomalia e verificarne il corretto funzionamento.

- **MDM.** Sui telefoni cellulari verrà installato l'agente per la gestione remota del dispositivo, necessario per garantire la sicurezza e l'integrità dei sistemi Aziendali. I dati trattati, le relative modalità ed i diritti della Persona Autorizzata sono esplicitati nella sezione **"Utilizzo della Rete Aziendale"**.
- **Anti-Virus.** Consente di rilevare e neutralizzare le minacce nel dispositivo utilizzando i database anti-virus e il servizio Security Network. Anti-Virus include i seguenti componenti: **Protezione**, **Scansione, Aggiornamento**.
- **Antifurto**. Questo componente protegge le informazioni sul dispositivo dall'accesso non autorizzato in caso di furto o smarrimento del dispositivo stesso. Consente di utilizzare i comandi per bloccare il dispositivo, localizzarlo (solo nel caso in cui l'utente abbia attivato l'opzione di localizzazione, o cancellare in remoto i dati dal dispositivo.
- **Filtro chiamate/messaggi di testo**. A seconda della modalità di funzionamento selezionata, "Filtro chiamate/messaggi di testo" è possibile bloccare le chiamate e i messaggi SMS indesiderati in entrata.
- **Protezione Web**. Questo componente blocca i siti dannosi progettati per distribuire codice malevolo. Blocca anche i siti Web contraffatti (di *phishing*) progettati per rubare informazioni riservate (ad esempio le password usate per l'*online banking* o sistemi *e-money*) ed ottenere l'accesso alle informazioni finanziarie dell'utente.
- **Sincronizzazione**. Consente di connettere un dispositivo mobile ad "Administration Server". La sincronizzazione consente di configurare in remoto le impostazioni dell'APP e del dispositivo mobile utilizzando i criteri di gruppo configurati in "Administration Console".
- **Quarantena**. Questo componente sposta i file rilevati nel corso della scansione del dispositivo o durante la protezione in tempo reale in un archivio dedicato. I file vengono memorizzati in Quarantena, in modo che non possano danneggiare il dispositivo. Quarantena consente di eliminare o ripristinare i file che sono stati spostati nell'archivio specifico.
- **Rapporti**. Questo componente consente di ottenere informazioni sull'esecuzione di Anti-Virus, "Filtro chiamate/messaggi di testo" e "Protezione Web" nel dispositivo mobile dell'utente. Il componente ordina i rapporti cronologicamente. Un rapporto può contenere al massimo 200 voci di eventi. Al superamento delle 200 voci nel rapporto, le meno recenti vengono sovrascritte dalle nuove voci.
- **Installazione software**: l'installazione di software oltre a quello di dotazione iniziale deve essere richiesta ed autorizzata esplicitamente dall'Ufficio Informatica e Sviluppo ICT.

6.1.6 Riconsegna dei telefoni cellulari

Gli Strumenti Informatici Aziendali, ed in particolare i telefoni cellulari e i loro accessori, devono essere considerati in tutto il loro ciclo di vita e, dunque, le regole di comportamento devono essere seguite anche quando diventano inservibili o, per qualsiasi causa, devono essere dismessi.

Nel seguito, come prescritto nel Provvedimento del Garante per la Protezione dei Dati Personali "Rifiuti di apparecchiature elettriche ed elettroniche (RAAE) e misure di sicurezza dei dati personali" del 13 ottobre 2008, si elencano le regole da rispettare per la dismissione dei telefoni cellulari, quando manifestano problemi anche parziali nel funzionamento (e devono essere resi al fornitore) ovvero non si intenda più utilizzarli, nonché quando vengono smarriti o illecitamente sottratti.

6.1.7 Restituzione/sostituzione

In caso di restituzione o sostituzione del cellulare, la Persona Autorizzata dovrà consegnare il

dispositivo ed i relativi accessori all'Ufficio Informatica e Sviluppo ICT secondo le modalità operative vigenti.

La riconsegna è formalizzata con l'utilizzo di moduli di sistema in vigore.

Prima della restituzione, la Persona Autorizzata deve mettere a disposizione dell'Ufficio di appartenenza i dati aziendali in esso contenuti e, quindi, provvedere a cancellare o comunque rimuovere eventuali Dati Personali e/o ogni altro documento e informazione inerente l'attività lavorativa.

Quanto sopra, tenuto conto del fatto che il supporto sarà formattato attraverso misure tecniche per la cancellazione sicura dei dati tramite programmi che provvedono a distruggere i dati ivi contenuti in modo criptograficamente sicuro e comunque a renderli totalmente irrecuperabili.

6.1.8 Furto/smarrimento

In caso di **furto o smarrimento**, la Persona Autorizzata deve denunciare immediatamente l'accaduto:

- All'Ufficio Informatica e Sviluppo ICT in modo che possano essere prese misure per ridurre i rischi;
- alle competenti Autorità di Pubblica Sicurezza. Copia della denuncia, comprendente come prassi tutti gli identificativi specifici dell'apparato oggetto del furto/smarrimento comprensivi del codice IMEI dovrà essere consegnata/inviata, entro e non oltre quattro giorni dall'evento, alla Segreteria Generale dell'Ente (che provvederà alla protocollazione e all'invio all'Ufficio Informatica e Sviluppo ICT).

6.2 Utilizzo della Rete Aziendale

6.2.1 Gestione delle credenziali per l'utilizzo di applicazioni tramite cellulari

Le credenziali di autenticazione per l'accesso agli applicativi aziendali che fossero fruibili tramite specifiche APP o la posta elettronica cui la Persona Autorizzata ha accesso in base alla sua funzione, vengono assegnate dall'Ufficio Informatica e Sviluppo ICT, dietro richiesta formale del Direttore / Dirigente competente e secondo le modalità operative in vigore, e consistono in un codice per l'identificazione (user id), associato ad una parola chiave riservata (password). La password dovrà essere modificata alla consegna del dispositivo, ovvero inserita.

E' vietata la comunicazione e/o divulgazione, in qualsiasi modo essa avvenga, della password, così com'è vietato lasciarla incustodita.

Si ricorda che la Persona Autorizzata non può condividere la propria password con altri e deve procedere alla sua modifica almeno ogni tre mesi. Nei sistemi che lo prevedono, la password non deve contenere riferimenti agevolmente riconducibili alla Persona Autorizzata. L'AdSP raccomanda che la password contenga almeno un carattere maiuscolo, uno minuscolo ed un carattere numerico (es. Abd123d4e1yz). Tali caratteristiche devono essere applicate quando il sistema lo consenta anche se non richieste automaticamente.

La Persona Autorizzata è responsabile di qualunque accesso effettuato alla Rete Aziendale, anche da terzi, utilizzando le sue credenziali di autenticazione. In caso la Persona Autorizzata dimentichi ovvero smarrisca le proprie credenziali di autenticazione, sarà dovere della stessa fare immediata segnalazione all'Ufficio Informatica e Sviluppo ICT. Inoltre, nel caso in cui sospetti un'effrazione, incidente, abuso o violazione della sicurezza e segretezza delle proprie credenziali di autenticazione, la Persona Autorizzata dovrà modificare immediatamente la password e segnalare l'accaduto all'Ufficio Informatica e Sviluppo ICT.

Nell'ipotesi di sospensione e/o revoca delle credenziali di autenticazione, le stesse verranno immediatamente disattivate dall'Ufficio Informatica e Sviluppo ICT. Come regola generale, le credenziali di autenticazione non utilizzate da più di sei mesi, saranno disattivate dall'Ufficio

Informatica e Sviluppo ICT, salvo casi specifici autorizzati.

E' buona pratica, ma costituisce anche una misura di sicurezza da tenere presente, NON utilizzare la medesima password per accedere a diversi sistemi, applicazioni, e/o sistemi esterni.

6.2.2 Utilizzo della Rete Aziendale e, in generale, di internet

L'accesso alla Rete Aziendale, quando consentito, è registrato come per tutti gli Strumenti Informatici Aziendali, ed avviene attraverso credenziali di autenticazione specifiche per ciascuna Persona Autorizzata e, ove possibile e necessario, da un accesso VPN nel caso di Device Mobili che accedono da fuori il perimetro aziendale (si veda il paragrafo 6.2.3 "Wi-Fi guest e VPN).

Trattandosi di uno strumento funzionale allo svolgimento della sola attività lavorativa, l'AdSP vanta un interesse legittimo a che la Rete Aziendale sia sottoposta a tecniche di filtraggio e monitoraggio che ne garantiscano la sicurezza.

Sul punto, si ricorda che l'AdSP ha installato sulla Rete Aziendale sistemi di registrazione degli accessi e sistemi di content filtering in grado di impedire l'accesso a siti non pertinenti con l'attività lavorativa o che offrono contenuti palesemente violativi del diritto d'autore.

In ogni caso, trattandosi di strumento di lavoro, alla Persona Autorizzata non è consentito, neanche al di fuori della rete aziendale, accedere a siti Internet o partecipare a chat-line, newsgroup o social network:

- superando o tentando di superare o disabilitando i sistemi di protezione e/o filtro eventualmente adottati dall'AdSP per bloccare l'accesso a determinati siti ed in ogni caso utilizzare siti o altri strumenti che realizzino tale fine;
- che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico, rilevante ai fini della realizzazione di una fattispecie di reato o che sia in qualche modo discriminatorio sulla base della razza, del colore della pelle, della fede religiosa, del sesso, della cittadinanza, dello stato civile, degli handicap, ovvero degli altri principi e valori statuiti al riguardo dalla legislazione nazionale ed europea, salvo quanto espressamente autorizzato di volta in volta dall'AdSP o per assolvere a richieste dell'autorità competente od ad obblighi di legge;
- per promuovere utile o guadagno personale nell'orario di lavoro e all'interno dei locali aziendali o tramite Strumenti Informatici Aziendali;
- per utilizzare l'accesso alla Rete Aziendale in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore;

Nel caso in cui la Rete Aziendale impedisca l'accesso a contenuti rilevanti per l'attività lavorativa (cd. falsi positivi), la Persona Autorizzata contatterà l'ufficio Informatica e Sviluppo ICT e/o le competenti funzioni tecniche espressamente indicate dal medesimo affinché crei un'eccezione temporanea o permanente per quel contenuto.

Gli accessi alla Rete Aziendale sono registrati, nel rispetto della normativa vigente. ADSP non monitora i log degli accessi, ma questi potrebbero essere conferiti, su richiesta, alle autorità aventi titolo (es. Polizia Giudiziaria).

6.2.3 Wi-Fi e VPN

L'amministrazione prevede accessi Wi-Fi nei locali di AdSP pertanto, le Persone Autorizzate, quando si trovano a rendere la prestazione lavorativa nei predetti locali, dovranno utilizzare prioritariamente tale modalità di accesso, ciò al fine di rendere l'utilizzo dell'apparato più efficiente sia dal punto di vista tecnico che economico.
Allo stesso fine si raccomanda di utilizzare anche fuori dai locali di AdSP, laddove possibile, reti Wi-Fi avendo cura di connettersi a reti protette da password per l'accesso (Abitazione, Hotel ...)

Tale buona prassi è particolarmente indicata al di fuori dell'Unione europea, stante i connessi maggiori costi.

La Persona Autorizzata, ove necessario, potrà richiedere l'abilitazione ad una **Virtual Private Network** (VPN) per l'accesso alla Rete Aziendale. Si ricorda che una volta attivata la VPN, tutta la navigazione verrà filtrata da sistemi più sopra descritti, in modo da impedire l'accesso a siti non pertinenti con l'attività lavorativa o che offrono contenuti palesemente violativi del diritto d'autore o delle leggi dello Stato.

6.3 Utilizzo della Posta Elettronica

6.3.1 Regole generali

La casella di Posta Elettronica Aziendale assegnata alla Persona Autorizzata è uno strumento di lavoro e deve essere utilizzata, anche attraverso dispositivi mobili, per motivi attinenti e collegati con l'attività lavorativa.

L'uso dell'indirizzo di Posta Elettronica Aziendale è, pertanto, ammesso per motivi attinenti all'attività professionale e tutti i messaggi in entrata e in uscita dagli indirizzi di Posta Elettronica Aziendale sono di proprietà dell'AdSP.

L'uso della casella di Posta Elettronica Aziendale per motivi personali è da ritenersi residuale ed eccezionale e la Persona Autorizzata dovrà periodicamente cancellare messaggi di natura personale eventualmente presenti nella propria casella di Posta Elettronica Aziendale;

Alla Persona Autorizzata, non è consentito:

- utilizzare l'indirizzo aziendale di posta elettronica per inviare e/o ricevere allegati contenenti filmati o brani musicali (es. mp3) non correlati all'attività lavorativa;
- inviare a soggetti esterni all'AdSP, tramite Posta Elettronica Aziendale, messaggi con in allegato file eseguibili (exe), salvo espressa autorizzazione dall'ufficio Informatica e Sviluppo ICT di AdSP;
- utilizzare la Posta Elettronica Aziendale in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore e in violazione alle Leggi dello Stato.

E' obbligatorio porre la massima attenzione nell'aprire i file attachment di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o FTP non conosciuti, avvisare sempre l'ufficio Informatica e Sviluppo ICT per i comportamenti della specie).

In considerazione dell'ambito di attività dell'AdSP, particolare cautela deve essere prestata dalla Persona Autorizzata in caso di ricezione e trasmissione all'esterno di file contenenti Dati Particolari o informazioni riservate, quali ad esempio i dati sensibili o ultrasensibili dei dipendenti o collaboratori. A tal fine, tali documenti e file devono essere sempre protetti con adeguate tecniche di cifratura, che possono essere richiesti dall'ufficio Informatica e Sviluppo ICT.

Non è consentito parimenti utilizzare la casella di posta elettronica personale per fini lavorativi, salvo espressa autorizzazione in caso di impossibilità della Persona Autorizzata di poter utilizzare l'account aziendale per inviare, ad esempio, a soggetti terzi documenti aziendali.

6.4 Controllo della Rete Aziendale

6.4.1 Tipologie di controllo

Obiettivo primario delle attività di presidio e controllo dei sistemi informatici è quello di proteggere il patrimonio aziendale e salvaguardare le informazioni rilevanti.

Gli incaricati delle competenti funzioni tecniche interne o esterne all'AdSP debitamente nominati, Gestori del Sistema, sono autorizzati a compiere interventi nella Rete Aziendale e sugli applicativi aziendali:

- diretti a garantire la sicurezza degli stessi sistemi, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware etc.);
- per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.);

- per finalità di salvaguardia del patrimonio, del know how e dei beni/strumenti dell'AdSP in dotazione alle Persone Autorizzate;
- per evitare che la continuità della normale attività operativa possa essere pregiudicata da azioni od omissioni delle Persone Autorizzate;
- per prevenire/accertare e di conseguenza potersi tutelare in giudizio l'amministrazione in caso di fatti illeciti e/o condotte/eventi aventi rilevanza penale e/o inadempimenti contrattuali, commessi dalle Persone Autorizzate e che possano arrecare danno all'AdSP.

I suddetti controlli sono generati da automatismi del sistema e non potranno, comunque, mai avere la finalità di verificare le abitudini e/o le opinioni delle Persone Autorizzate, né finalità di controllo a distanza dei lavoratori. La persona autorizzata, qualora si renda conto di un'anomalia nel funzionamento o nei consumi è tenuta a segnalarlo immediatamente all'ufficio ICT che svolgerà tutte le opportune verifiche. Parimenti, qualora sulla base dei predetti automatismi l'ufficio ICT noti anomalie ne verificherà le ragioni previo confronto con la Persona Autorizzata. Eventuali anomalie rispetto al normale uso e funzionamento saranno segnalate direttamente dalla Persona Autorizzata, qualora se ne avveda, o dai gestori del sistema che provvederanno alle verifiche del caso informando la Persona Autorizzata.

I controlli posti in essere dall'AdSP potranno avere ad oggetto, oltre a quanto sopra, anche il rispetto delle corrette modalità di utilizzo da parte delle Persone Autorizzate all'uso degli Strumenti Informatici Aziendali in loro dotazione, nonché della Rete Aziendale e della Posta Elettronica Aziendale, sempre e solo per le suddette precipue finalità organizzative e/o di sicurezza.

La stessa facoltà di controllo sempre ai fini della sicurezza del sistema informatico aziendale e del patrimonio dell'AdSP nonché per garantire la normale operatività, si estende anche in caso di assenza prolungata o impedimento della Persona Autorizzata.

6.4.2 **Controllo ordinario**

L'AdSP si riserva, in casi di ripetuti tentativi di accesso a contenuti non autorizzati della Rete Aziendale, non preceduti da una richiesta di accesso, il diritto di svolgere un controllo ordinario sui server aziendali, per mezzo delle competenti funzioni incaricate, circa l'uso della Rete Aziendale, in conformità a quanto stabilito nel presente Regolamento.

Secondo un criterio graduale ed alla luce dei principi di pertinenza e non eccedenza, in caso di necessità, gli addetti dell'AdSP e/o delle competenti funzioni tecniche espressamente indicate dall'AdSP, effettueranno in via ordinaria un controllo preliminare su dati aggregati, riferiti all'intera Rete Aziendale.

Il controllo anonimo aggregato può concludersi con un avviso generalizzato a tutti i dipendenti relativo ad attività anomale, con l'invito ad attenersi scrupolosamente alle istruzioni impartite.

6.4.3 **Controllo straordinario**

Al fine di assicurare il rispetto del presente Regolamento, nonché della normativa vigente, sempre nel rispetto del sopracitato criterio graduale ed alla luce dei principi di pertinenza e non eccedenza – ove nel corso del Controllo ordinario, descritto nel capitolo precedente, dovessero riscontrarsi anomalie ovvero dovesse emergere, dai dati e dalle informazioni rilevate, il sospetto del verificarsi, anche potenziale, di fatti illeciti e/o condotte/eventi aventi rilevanza penale e/o inadempimenti contrattuali, il Gestore del Sistema segnalerà quanto rilevato al datore di lavoro.

In ogni caso, non verrà svolta alcuna delle seguenti attività:

- lettura e registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
- riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dalla Persona Autorizzata (al di fuori di quanto in obbligo normativo) ;
- lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;

- analisi occulta di Strumenti Informatici Aziendali affidati in uso.

7. INFORMAZIONI SUL TRATTAMENTO DATI

I dati saranno trattati, nel rispetto dei principi e dei limiti di cui al D.Lgs. 196/2003 e del GDPR, al solo fine di monitorare il corretto funzionamento ed utilizzo degli apparati ed i consumi. Il trattamento avverrà con l'utilizzo di strumenti e procedure idonee a garantire la sicurezza e la riservatezza e sarà effettuato anche attraverso l'ausilio di strumenti informatici.

Oltre che per le finalità sopra descritte i dati personali potranno essere altresì trattati per adempiere agli obblighi previsti da leggi, regolamenti o normative comunitarie, nonché da disposizioni delle Autorità di vigilanza del settore.

I dati memorizzati non saranno diffusi (cioè messi a disposizione di soggetti indeterminati), e saranno trattati secondo le modalità e i limiti previsti nel presente regolamento dal Gestore del sistema nonché da Telecom Italia Spa per quanto riguarda i dati di telefonia, come da informativa dal medesimo rilasciata sottoscritta dalla Persona Autorizzata al momento della consegna della SIM aziendale.

La Persona Autorizzata potrà esercitare i diritti di cui all'art. 13 del GDPR, ricordandosi tuttavia che, qualora non vi fosse consenso al trattamento dei dati o fosse revocato, ciò potrebbe comportare la mancata assegnazione o il ritiro dell'apparato o, comunque, l'impossibilità di attivare e fornire i servizi richiesti.

8. SANZIONI

E' fatto obbligo a tutte le Persone Autorizzate di osservare le disposizioni e regole di condotta portate a conoscenza con il presente Regolamento.

In particolare, la violazione delle previsioni del presente Regolamento da parte delle Persone Autorizzate potrà quindi determinare l'applicazione delle sanzioni previste dal codice civile e dallo statuto dei lavoratori, oltre che dal contratto in essere.

9. CICLO DI EMISSIONE

Rev.	Data			
1.0	24/07/2019	Redatto	Controllato	Approvato
Funzione		Responsabile RTD – Rossana Varna	DPO- Tania Valle	Datore di Lavoro – Marco Sanguineri
Firma				