# REGOLE PER L'UTILIZZO DI STRUMENTAZIONI INFORMATICHE

## 1. Oggetto, campo di applicazione e principi generali

Il presente documento disciplina l'utilizzo delle risorse informatiche, della posta elettronica e di Internet messi a disposizione dall'Agenzia Regionale per lo sviluppo rurale - ERSA. Stabilisce inoltre i controlli che l' ERSA può effettuare per verificarne il corretto utilizzo.

Esso si applica ai dipendenti dell'Amministrazione regionale assegnati all'ERSA nonché a tutti coloro che, a vario titolo, sono abilitati ad utilizzare risorse informatiche dell'Agenzia.

Il documento, nell'indicare il corretto utilizzo delle risorse informatiche, mira a garantire l'integrità del sistema informativo, nel rispetto delle disposizioni dettate dal Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 «relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)» e dal decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE) e all'applicazione delle misure di sicurezza ai sensi della Circolare AgID 17 marzo 2017, n. 1/2017 recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni".

Gli strumenti informatici forniti dall'Agenzia sono messi a disposizione del personale per svolgere l'attività lavorativa. L'utilizzo di tutti gli strumenti informatici deve ispirarsi ai principi di diligenza e correttezza impliciti nel rapporto di lavoro.

Il presente documento si pone come scopo principale quello di:
- disciplinare l'utilizzo delle risorse informatiche fornite dall'Agenzia nell'ottica di una maggiore efficacia, produttività e corretto utilizzo;
- fornire informazioni sui controlli che potranno essere effettuati sull'utilizzo degli strumenti di lavoro;
- garantire la sicurezza ed il rispetto della privacy, con riferimento alle misure di sicurezza imposte dalle normative vigenti sul trattamento dei dati personali;
- ridurre i rischi derivanti da un utilizzo non corretto delle risorse informatiche.

La responsabilità nell'utilizzo delle risorse è a carico del soggetto che le ha in dotazione. Il monitoraggio e il controllo degli strumenti affidati per lo svolgimento della prestazione lavorativa saranno effettuati nel rispetto dei principi di:
- necessità: i dati trattati durante l'attività di controllo devono essere sempre e soltanto quelli strettamente necessari a perseguire le finalità di verifica;
- trasparenza e correttezza: le caratteristiche essenziali dei trattamenti svolti mediante monitoraggio degli strumenti affidati per la prestazione lavorativa devono essere rese note ai dipendenti;
- pertinenza e non eccedenza: i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime, nella misura meno invasiva possibile.

## 1.2. Definizioni

Ai fini del presente documento s'intende per:
a) <<autenticazione informatica>>: l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
b) <<Codice Identificativo personale>>: il dato, componente di una Credenziale di autenticazione in possesso di una persona, da questa conosciuto o ad essa univocamente correlato, utilizzato per l'autenticazione informatica (Chiave di Login);
c) <<Credenziale di autenticazione>>: i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

d) <<Parola chiave>>: 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. È altresì nota come Password;
e) <<Posta elettronica>>: messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso la rete dell'Amministrazione o una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza;
f) <<Chat>>: software che consente la conversazione contemporanea fra utenti online, tramite lo scambio di messaggi di messaggi di testo, o multimediali, visualizzati sullo schermo in tempo reale;
g) <<Cracking Programs>>: software idonei a violare le protezioni o le password di altri software;
h) <<Malware, Spyware, Adware>>: software che si installano sul computer, con o senza la consapevolezza dell'utente, e che svolgono azioni di controllo sull'attività e sulla navigazione in internet svolta dal computer. Questi software possono inviare pubblicità e messaggi non richiesti;
i) <<VPN (Virtual Private Network)>>: lo scopo delle reti VPN è quello di offrire l'accesso alla rete regionale sfruttando reti condivise pubbliche, mediante un accesso internet privato o regionale per l'instradamento tramite IP equivalente a un'infrastruttura fisica di rete (ossia con collegamenti fisici) dedicata;
j) <<AdS (Amministratori di sistema)>>: tecnico specializzato che si occupa dell'installazione, configurazione, gestione/manutenzione, aggiornamento e monitoraggio di un sistema operativo e, più in generale, di uno o più sottosistemi di un sistema informatico;
k) <<Dominio>>: un insieme di computer di una rete che vengono amministrati con regole e procedure comuni;
l) <<Protezione crittografica>>: metodo per rendere un messaggio "offuscato" in modo da non essere comprensibile/intelligibile a persone non autorizzate a leggerlo, ovvero non in possesso dei requisiti per la decrittazione.

## 2. Utilizzo delle risorse hardware e software

### 2.1. Affidamento ed utilizzo

Le risorse hardware e software sono affidate dall'Agenzia a ciascun dipendente, che ha il compito di utilizzarle con diligenza. È facoltà dell' ERSA revocarne in qualsiasi momento l'affidamento. I dispositivi informatici (PC, stampanti, memorie USB, memorie flash, periferiche, tablet) sono ad uso esclusivo dei dipendenti.

I dispositivi vanno custoditi con la massima diligenza, sia in sede sia fuori sede, e devono essere utilizzate password (o un segno o un PIN) per l'accesso.

Non è consentito installare in autonomia software non compresi nell'elenco di quelli autorizzati per non pregiudicare la funzionalità del dispositivo o compromettere la riservatezza dei dati in esso contenuti. Le richieste di installazione di software non presenti nell'elenco o le proposte di aggiornamento dello stesso vanno sottoposte alla valutazione del Servizio competente in materia di sistemi informativi mediante richiesta CRM (Gestione postazioni di lavoro, per il tramite del viceconsegnatario).

Non è consentito disinstallare o alterare applicazioni installate sul dispositivo.

E' compito del dipendente, assegnatario di dispositivi informatici:
- utilizzare in modo appropriato e responsabile i dispositivi hardware e software a lui affidati;
- assicurare periodicamente il salvataggio dei dati nelle specifiche aree di archiviazione della rete regionale messe a disposizione del dipendente e del suo Servizio;
- individuare, in accordo con il Direttore di riferimento, i dati con particolari requisiti di riservatezza (dati rilevanti) e quelli ai quali va applicata la protezione crittografica;
- impostare e utilizzare il blocco automatico dello schermo del dispositivo dopo un predefinito periodo di inattività;
- adottare adeguate misure di sicurezza nel caso di utilizzo dei beni al di fuori delle sedi dell'ERSA.

Al dipendente non è consentito:
- utilizzare le risorse per scopi estranei all'attività lavorativa, né modificare le configurazioni;
- installare dispositivi che compromettano l'integrità, l'operatività e la sicurezza delle risorse hardware e software e, più in generale, del sistema informativo regionale;

- installare dispositivi atti ad intercettare, falsificare, alterare o sopprimere il flusso dei dati che transitano nella rete regionale.

L'accesso via VPN è consentito unicamente ai personal computer portatili dell'Agenzia. Quindi, a titolo esemplificativo ma non esaustivo, sono esclusi dall'utilizzo della VPN tutti i dispositivi personali e i cosiddetti dispositivi mobili (smartphone, tablet, ecc..).

Fatte salve le abilitazioni di ciascun utente, l'installazione di ulteriori dispositivi hardware o software può avvenire solo a seguito di autorizzazione del Servizio competente in materia di sistemi informativi.

In caso di furto o smarrimento di un dispositivo hardware, rilevato all'interno della sede di lavoro, il dipendente deve dare comunicazione immediata al proprio Responsabile e al Viceconsegnatario, il quale provvederà a presentare denuncia formale presso l'Ufficio di Pubblica sicurezza (Polizia o Carabinieri) più vicino. In caso di evento rilevato al di fuori della sede di lavoro, il dipendente deve procedere con denuncia formale presso i competenti organi di polizia e fornire copia della denuncia al Viceconsegnatario e al proprio Responsabile.

### 2.2 Controlli sui dispositivi informatici

In ottemperanza alla Circolare AgID 17 marzo 2017, n. 1/2017 recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni", al fine di garantire la sicurezza e non compromissione dei dispositivi informatici connessi alla rete regionale, sono previste scansioni automatiche dei software installati sui dispositivi aziendali.

L'elenco dei software installati potrà essere confrontato con l'elenco dei software autorizzati, al fine di identificare installazioni non autorizzate.

Sono previste inoltre azioni di ricerca di vulnerabilità presenti sui sistemi regionali con strumenti automatici. Tali informazioni saranno impiegate nel processo di gestione dei rischi, per l'implementazione di opportune contromisure o per l'accettazione dei rischi derivanti.

Sui dispositivi che lo consentono è installato uno strumento atto a rilevare la presenza e bloccare l'esecuzione di malware. (cd. Antivirus).

### 2.3. Utilizzo di supporti rimovibili

Sono intesi come rimovibili supporti quali dvd, memorie flash, memorie di massa esterna, memorie USB, ecc.

Ogni dipendente può impiegare, per le sole necessità di lavoro, supporti di memorizzazione per memorizzare e/o trasferire dati ed informazioni. Non è consentito al dipendente, nell'utilizzo dei supporti forniti dall'Agenzia, memorizzare su di essi files non aventi attinenza con la propria attività lavorativa.

In caso di dismissione di un supporto rimovibile è necessario cancellare in maniera adeguata le informazioni presenti oppure distruggere il supporto stesso, per evitare che il contenuto possa essere recuperato, anche dopo la rimozione dei dati.

In presenza di dati inerenti l' ERSA su supporti rimovibili, il dipendente deve:
- trattarli con cautela per evitare ogni possibilità di comunicazione non autorizzata o diffusione accidentale delle informazioni in essi contenute;
- custodirli in archivi chiusi a chiave;
- limitare la permanenza dei dati sul supporto al solo tempo necessario allo svolgimento dell'attività;
- conservare i dati originali su un supporto diverso da quello rimovibile.

Sistemi automatici installati sui dispositivi informatici effettueranno la scansione dei contenuti dei supporti rimovibili al fine di prevenire la diffusione di malware e virus sui sistemi informatici dell'Amministrazione.

### 2.4. Amministratori di sistema

La gestione dell'amministratore di sistema dell'Agenzia è effettuata esclusivamente da personale dalla società INSIEL.

## 3. Posta elettronica

### 3.1. Utilizzo della casella

La casella di posta elettronica, assegnata ad ogni dipendente, è uno strumento di lavoro che di norma è codificato nel seguente modo: nome.cognome@ersa.fvg.it.

La casella è uno strumento di lavoro strettamente personale, il cui accesso è consentito esclusivamente al titolare della stessa o al personale da lui autorizzato e agli amministratori di sistema espressamente autorizzati.

Il dipendente, in qualità di assegnatario della casella di posta elettronica, è responsabile del corretto utilizzo della stessa, e, in particolare, ha il diritto di:

- utilizzare la posta per scopi lavorativi;
- utilizzare la posta per comunicazioni tra i lavoratori dipendenti (posta interna regionale, ad esempio relazioni sindacali, comunicazioni del Circolo Dipendenti, eccetera).

Il dipendente, inoltre, è tenuto a:

- leggere quotidianamente la posta, qualora in servizio, ed a rispondere alla stessa in tempi ragionevoli;
- ottimizzare lo spazio occupato dalla propria casella di posta, cancellando i messaggi non più necessari e archiviando i messaggi di meno frequente consultazione.

Non è consentito:

- inviare o memorizzare messaggi personali, pubblicitari, promozionali o messaggi di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione ed appartenenza sindacale e/o politica;
- registrarsi a siti, mailing list, bacheche elettroniche, forum o dibattiti non professionali, i cui contenuti esulino dall'attività lavorativa o da scopi di informazione, formazione e/o aggiornamento;
- inviare messaggi in modo anonimo o modificando la reale identità del mittente;
- utilizzare il proprio indirizzo di posta in contesti nei quali possa ingenerare confusione fra il ruolo istituzionale e l'esercizio della libertà di pensiero;
- l'utilizzo delle caselle di posta elettronica regionale per comunicazioni di carattere personale.

In caso di arrivo di messaggi non attinenti al lavoro e non sollecitati, il dipendente dovrà segnalare il problema alle strutture competenti dell'Amministrazione.
La posta elettronica non deve essere utilizzata per inviare documenti che siano stati esplicitamente designati dal Responsabile dell'ufficio come "di natura strettamente riservata". Il messaggio infatti potrebbe essere ricevuto da destinatari diversi da quelli a cui è diretto, non venire recapitato o essere distrutto, per problemi tecnici imprevedibili; inoltre, per sua intrinseca natura tecnica, è leggibile da chiunque durante il suo percorso nella rete Internet prima di giungere al destinatario.

L'accesso alla casella di posta elettronica, con dispositivi informatici non forniti dall'Amministrazione, è consentito solo tramite accesso alla webmail. E' fatto divieto di memorizzare credenziali di accesso su dispositivi mobili personali.

### 3.2. Destinatari dei messaggi

Il dipendente deve prestare particolare cura:

- nella selezione dei destinatari, in particolare nell'invio per conoscenza a soggetti non direttamente interessati all'argomento;
- nell'utilizzare automatismi di risposta o inoltro;
- nell'uso di stampanti di piano o accessibili a più dipendenti, per evitare che il messaggio sia letto da altri.

In presenza di molteplici destinatari, il dipendente è tenuto a:

- non inviare messaggi a destinatari o gruppi di destinatari che, per l'attività svolta, non siano direttamente interessati all'argomento o che non siano le persone competenti a trattare il problema in oggetto;
- utilizzare le liste di destinatari fornite dall'Amministrazione solo se è autorizzato all'uso;

- utilizzare con cautela la funzione di invio per conoscenza nascosta (Ccn);
- utilizzare gli indirizzi di posta istituzionale (Strutture, Servizi, Direzioni) solo per scopi lavorativi.

### 3.3. Linee guida per l'indicazione delle generalità del mittente in calce alle e-mail

Nella scrittura di e-mail inviate all'esterno dell'Amministrazione dovrà essere apposto in calce un testo, su più righe, così strutturato:
1. nome e cognome del mittente scritto in grassetto;
2. indicazione dell'Ente di appartenenza (Agenzia regionale per lo sviluppo rurale – ERSA)
3. indicazione del Servizio e/o P.O. di appartenenza;
4. indirizzo della propria sede di lavoro;
5. CAP e Città (eventuale sigla della provincia se la città non è capoluogo);
6. numero di telefono fisso (diretto o del centro di segreteria oppure del centralino);
7. numero di fax assegnato (personale o del centro di segreteria);
8. eventuale numero di cellulare assegnato (ove ritenuto opportuno comunicarlo);

Dopo il testo di cui sopra dovranno essere riportate le seguenti diciture:
AVVISO DI RISERVATEZZA
"Informazioni riservate possono essere contenute nel messaggio o nei suoi allegati. Se non siete i destinatari indicati nel messaggio, o responsabili per la sua consegna alla persona, o se avete ricevuto il messaggio per errore, non dovete trascriverlo, copiarlo o inviarlo a nessuno. In tal caso, dovete cancellare/distruggere il messaggio ed i suoi allegati. Grazie."
CONFIDENTIALITY NOTICE
"Confidential information may be contained in this message or in its attachments. If you are not the addressee indicated in this message, or responsible for message delivering to that person, or if you have received this message in error, you may not transcribe, copy or deliver this message to anyone. In that case, you should delete/destroy this message and its attachments. Thank you".

Nel caso di assenza del dipendente è opportuno inserire in calce alla mail l'informazione "Out of office" con l'indicazione eventuale del referente a cui rivolgersi durante l'assenza dal servizio.

### 3.4. Contenuto dei messaggi

Il dipendente deve prestare attenzione:
- all'invio di messaggi elettronici, affinché non vengano inserite inconsapevolmente informazioni dannose o pregiudizievoli per la sicurezza dell'Amministrazione. In particolare, va usata la massima cautela nel rinvio a pagine Internet, che per loro natura potrebbero contenere delle informazioni per risalire alla modalità di accesso utilizzata;
- a non inviare informazioni il cui livello di riservatezza potrebbe essere non compatibile con il livello di sicurezza offerto dallo strumento;
- ai file allegati al messaggio di posta elettronica, controllandone accuratamente il contenuto;
- all'attendibilità dell'identità del mittente, qualora sia necessaria la certezza della stessa, essendo relativamente facile contraffare il mittente di una e-mail.

## 4. Internet

### 4.1. Navigazione

Il dipendente è tenuto ad utilizzare il servizio Internet per motivi legati alla sua attività lavorativa, in modo responsabile e secondo buona fede, nel rispetto della sicurezza del sistema informativo dell'Amministrazione.

Non è consentito:

- modificare le impostazioni assegnate in relazione all'accesso alla rete, fatte salve le specifiche necessità operative connesse alle mansioni attribuite al dipendente stesso;
- utilizzare browser diversi da quello preinstallato;
- effettuare lo scarico gratuito o a pagamento dalla rete di file di qualunque formato (ad esempio filmati, musica, programmi, ecc.), che non siano inerenti allo svolgimento delle attività lavorative o di formazione, informazione e/o aggiornamento;
- effettuare, per fini diversi dalla propria attività lavorativa, qualunque genere di transazione finanziaria, comprese le operazioni di remote banking e gli acquisti online;
- accedere a siti Internet che abbiano un contenuto contrario a norme di legge e di tutela dell'ordine pubblico, rilevanti ai fini della configurazione di un reato;
- esprimere opinioni su Internet spendendo il nome dell'Amministrazione, per scopi estranei allo svolgimento dell'attività lavorativa. Il dipendente, durante la navigazione finalizzata alla propria attività lavorativa, è tenuto a leggere con attenzione qualsiasi finestra, pop-up o avvertenza prima di proseguire nella navigazione, per evitare di accettare condizioni contrattuali o di aderire a delle iniziative di cui non si abbia piena e responsabile consapevolezza;
- disabilitare i sistemi adottati dall'Amministrazione per bloccare l'accesso ad alcuni siti ed in ogni caso utilizzare o detenere programmi utilizzabili per cracking (cracking programs).

### 4.2. Social media

Non sono ammessi comportamenti atti a:
- divulgare informazioni senza previa autorizzazione formale;
- incidere negativamente sull'immagine dell'Amministrazione;
- intervenire sui media per conto dell'Amministrazione senza previa autorizzazione formale.

### 4.3. Graduazione dei controlli

L'Amministrazione regionale ha diritto di configurare sistemi o utilizzare filtri che prevengano determinate operazioni reputate inconferenti con l'attività lavorativa, quali l'upload o l'accesso a determinati siti (inseriti in una black list) e/o il download di file o di software aventi particolari caratteristiche (dimensionali o di tipologia di dato).

Si informa, inoltre, che tutto il traffico viene registrato su log che non vengono direttamente analizzati, ma conservati in modo che possano essere messi a disposizione, se ufficialmente richiesto, dell'autorità giudiziaria e/o di polizia a fine di indagini.

L'Amministrazione regionale si riserva di effettuare controlli sull'utilizzo del servizio Internet al fine di garantire la funzionalità della rete e la fruibilità dei servizi informatici da parte di tutti i dipendenti. Ogni controllo sarà comunque effettuato nel rispetto dei principi di pertinenza e non eccedenza e sarà eseguito, in via preliminare, su dati aggregati riferiti all'intera struttura dell'Agenzia.

Successivamente potrà essere eseguito su aree aggregate per ufficio/immobile. Il controllo anonimo potrà concludersi con un avviso generalizzato relativo ad un rilevante utilizzo anomalo degli strumenti forniti dall'Amministrazione e con l'invito ad attenersi scrupolosamente ai compiti assegnati e istruzioni impartite.

L'avviso potrà essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia.

L'esito del controllo potrà essere un avviso generalizzato relativo ad un utilizzo anomalo delle risorse di rete.

### 4.4. Conservazione dei dati

Per ragioni di sicurezza del sistema i dati personali relativi agli accessi ad Internet e al traffico telematico vengono conservati per un periodo massimo di 30 giorni, trascorso il quale vengono cancellati automaticamente.

Un eventuale prolungamento del tempo di conservazione sarà eccezionale e avrà luogo solo in relazione:
- ad esigenze tecniche o di sicurezza del tutto particolari;

- all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

## 5. Accesso alla rete

### 5.1. Credenziali di autenticazione

A ogni dipendente viene assegnato un profilo di accesso che caratterizza le modalità con cui possono essere utilizzate le risorse del sistema informativo dell'Amministrazione.

Al profilo di ciascun dipendente è associato un codice identificativo personale e una parola chiave o altro sistema messo a disposizione dall'Amministrazione.

Il codice identificativo personale è costituito, di norma, dal numero di matricola del dipendente.

La parola chiave associata al codice identificativo personale è conosciuta solo dal dipendente e garantisce la riservatezza dell'accesso alle risorse.

Il trattamento di dati personali è consentito agli incaricati che, a tal fine, sono dotati di credenziali di autenticazione che abilitano al trattamento informatico dei dati.

L'abilitazione del computer a trattare i dati utilizzando le credenziali di autenticazione avviene mediante una procedura di "login" che prevede l'immissione del proprio codice identificativo personale e della parola chiave.

Nel momento in cui viene terminata o sospesa l'attività lavorativa sul computer il dipendente è tenuto a disabilitare le proprie credenziali mediante una procedura di "logout" che consiste nell'esecuzione dei comandi standard del sistema operativo di "disconnessione" o di "chiusura sessione".

Al fine di impedire utilizzi impropri del PC e, in particolare, il trattamento di dati da parte di persone non autorizzate, è fatto divieto di lasciare incustodito il computer fintanto che è abilitato con le proprie credenziali. In caso di allontanamento temporaneo dal proprio posto di lavoro è fatto obbligo al dipendente di utilizzare la procedura standard del sistema operativo di "blocca computer", innescata dalla sequenza di tasti CTRL-ALT-CANC.

È altresì prescritto di mantenere attiva sul proprio posto di lavoro la funzione standard del sistema operativo di "salvaschermo", associata alla parola chiave, con un tempo di attivazione automatica non superiore a 15 minuti.

### 5.2. Collegamento di dispositivi alla rete regionale

Sono collegabili alla rete regionale solo i dispositivi approvati dal Servizio competente in materia di sistemi informativi mediante richiesta CRM.

### 5.3. Accesso ai servizi informatici

Ogni dipendente ha la facoltà di accedere ai servizi informatici di propria competenza, a partire da qualsivoglia stazione di lavoro, utilizzando le credenziali di autenticazione. Pur tuttavia, l'accesso ai servizi informatici attraverso risorse hardware e software non di proprio affidamento è consentito solo con l'assenso del diretto interessato, oppure è regolamentato da norme di condivisione delle risorse informatiche specifiche dell'Ufficio di appartenenza, emanate dal Responsabile dell'ufficio stesso.

Non è consentito attivare dei meccanismi di blocco al momento dell'accensione del computer, basati sull'utilizzo di specifiche parole chiave (ad esempio, la password sul BIOS).

### 5.4. Dispositivi informatici non forniti dall'Amministrazione

Al dipendente non è consentito:
- collegare dispositivi informatici non forniti dall'Amministrazione alla rete regionale, compreso l'utilizzo di VPN;

• memorizzare informazioni relative all'Amministrazione su dispositivi informatici non gestiti dall'Amministrazione stessa, ivi comprese le credenziali di accesso;
• installare su dispositivi informatici non forniti dall'Amministrazione software dell'Amministrazione, se non espressamente e preventivamente autorizzati.

L'accesso alla casella di posta elettronica, con dispositivi informatici non gestiti dall'Amministrazione, è consentito solo tramite accesso alla webmail.

### 5.5 Disposizioni particolari per dispositivi mobili

È compito del dipendente, assegnatario di un dispositivo mobile:
• impostare e utilizzare il blocco automatico dello schermo del dispositivo dopo un predefinito periodo di inattività;
• utilizzare una password (o un segno o un PIN) per l'accesso al dispositivo;
• non disinstallare o alterare applicazioni installate sul dispositivo dell'Amministrazione;
• limitare la permanenza dei dati sul supporto al solo tempo necessario allo svolgimento dell'attività.

### 5.6. Disposizioni per la costruzione, l'utilizzo e la gestione delle parole chiave

La parola chiave personale, associata al codice identificativo personale, è quel componente, posseduto da ogni dipendente, che salvaguarda i privilegi di accesso da utilizzi illeciti. La parola chiave è assegnata al dipendente contestualmente alle credenziali di autenticazione. Il dipendente, al primo utilizzo, ha l'obbligo di sostituirla con una da lui scelta. A tal fine dovrà avvalersi della procedura standard del sistema operativo "cambia password".

È proibita la comunicazione via e-mail, verbale o di qualunque altro tipo, della parola chiave, anche nei confronti dei tecnici informatici preposti all'assistenza.

La parola chiave deve essere conosciuta solo dal dipendente, e pertanto non può considerarsi come chiave di gruppo. Non va annotata accanto alla stazione di lavoro o riferita a colleghi, amministratori di sistema o tecnici che eseguono interventi. Ogni inadempienza in tal senso può essere risolta procedendo alla modifica della parola chiave.

Il dipendente ha facoltà di cambiare la parola chiave in qualunque momento. A tal fine potrà avvalersi della procedura standard del sistema operativo "cambia password".

La parola chiave deve:
- avere una lunghezza minima di 8 caratteri, una certa complessità ed una validità massima di 6 mesi;
- essere diversa dal codice identificativo personale, dal cognome/nome del dipendente e dalla sua matricola o da elementi a lui facilmente riconducibili;
- essere priva di spazi vuoti in qualsiasi posizione.

### 5.7. Accesso al sistema in caso di impedimento del dipendente

Premesso che il Responsabile per la custodia delle credenziali di autenticazione è la società concessionaria INSIEL S.p.A., in caso di prolungata assenza o impedimento del dipendente che renda indispensabile e indifferibile intervenire sul sistema, per improrogabili necessità legate all'attività lavorativa, è facoltà dell'Amministrazione accedere con le credenziali del dipendente previa comunicazione al medesimo.

In tal caso il dipendente sarà tempestivamente informato e al suo rientro avrà facoltà di modificare la password anche prima della scadenza prevista.

# Elenco firmatari

*ATTO SOTTOSCRITTO DIGITALMENTE AI SENSI DEL D.P.R. 445/2000 E DEL D.LGS. 82/2005 E SUCCESSIVE MODIFICHE E INTEGRAZIONI*

Questo documento è stato firmato da:

*NOME: ANDREA COMACCHIO*
*CODICE FISCALE: CMCNDR61R21A703F*
*DATA FIRMA: 22/01/2020 10:32:37*
*IMPRONTA: A6638627B91E5D01ED7C188D975AE8C61F66E50D97CCD69F0ACF3F0C919EF269*
*1F66E50D97CCD69F0ACF3F0C919EF2694F679B2E563113E5D38FD529DC66E4AA*
*4F679B2E563113E5D38FD529DC66E4AA33C4C2CE293D8AC755DFED78F01C093E*
*33C4C2CE293D8AC755DFED78F01C093ED308373C4BB1D11FC2CCAE1FB04A2C03*