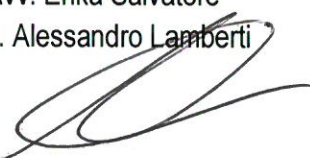


REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI AZIENDALI

STATO DEL DOCUMENTO	Emesso da:	Verificato da:
Identificazione: PO-19	Ufficio Legale Responsabile Sistemi informativi	Responsabile Ufficio Legale Presidente del Consiglio di Amministrazione
	Avv. Erika Salvatore Antonino Campo  	Avv. Erika Salvatore Avv. Alessandro Lamberti 
Approvata dal Consiglio di Amministrazione in data 10/07/2023		

Lista delle modifiche			
Identificazione	Revisione	Data	Tipo di modifica
PO-19	0	10/07/23	Prima emissione

INDICE

1.	SCOPO	4
2.	AMBITO DI APPLICAZIONE	5
3.	RIFERIMENTI	5
4.	DEFINIZIONI	5
5.	DISPOSIZIONI IN MERITO AGLI OBBLIGHI DEI DESTINATARI CON RIGUARDO ALLE MODALITÀ D'USO DEGLI STRUMENTI AZIENDALI	7
5.1	NORME DI COMPORTAMENTO	7
5.1.1	COMPORTAMENTO PROFESSIONALE	7
5.1.2	CUSTODIA, UTILIZZO E RESTITUZIONE DEGLI STRUMENTI AZIENDALI	7
5.1.3	MEMORIZZAZIONE E PROTEZIONE DEI DATI	9
5.1.4	GESTIONE DELLE CREDENZIALI DI ACCESSO	9
5.1.5	SOTTRAZIONE ALLA VISTA DELLE INFORMAZIONI SU SCHERMO	10
5.1.6	UTILIZZO DEI SISTEMI DI RIPRODUZIONE	11
5.2	UTILIZZO DEGLI STRUMENTI AZIENDALI E POSTAZIONI DI LAVORO	11
5.2.1	STRUMENTI DI REGISTRAZIONE DEGLI ACCESSI	11
5.2.2	POSTAZIONE DI LAVORO	11
5.2.3	INTERNET	11
5.2.4	INTRANET	12
5.2.5	POSTA ELETTRONICA AZIENDALE	13
5.2.6	SOFTWARE	15
5.2.7	ANTIVIRUS	16
5.2.8	TELEFONI / TABLET	17
5.2.9	CONTROLLI DA PARTE DELL'M4	17
5.2.10	CONSERVAZIONE	19
5.2.11	ISTRUZIONI IN CASO DI CESSAZIONE DEL RAPPORTO DI LAVORO O DI COLLABORAZIONE	19
5.2.12	VIOLAZIONI E SANZIONI	19
5.2.13	OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI	20
5.2.14	ENTRATA IN VIGORE DEL REGOLAMENTO E PUBBLICITÀ	20
5.2.15	MODIFICHE E AGGIORNAMENTI	20
5.2.16	DIFFUSIONE	20

1. SCOPO

SPV Linea M4 Spa (di seguito "**M4**"), per esclusive finalità lavorative/professionali, può mettere a disposizione mezzi informatici/telematici e l'accesso a Internet, quali strumenti di ricerca, archiviazione e lavoro, nonché strumenti di comunicazione, e di condivisione di informazioni strettamente lavorativi (es. posta elettronica, accesso alla rete aziendale da remoto, etc.).

M4 ha deciso, quindi, di adottare il presente Regolamento per l'utilizzo degli strumenti aziendali (di seguito "**Regolamento**") al fine di fornire un quadro preciso di indicazioni ai Lavoratori, e a tutti gli altri Destinatari (definiti *infra, sub* §2), in merito alla modalità di funzionamento degli Strumenti Aziendali (definiti *infra, sub* §4) loro assegnati o da essi comunque utilizzati, e dunque codificare il *set* di regole di comportamento da rispettare per un corretto utilizzo dei predetti Strumenti Aziendali, onde evitare problemi, disservizi e maggiori costi (di manutenzione o di altro tipo) ovvero rischi e/o minacce alla sicurezza dei sistemi e/o dei dati in essi contenuti, con particolare riguardo ai dati personali e/o al patrimonio dell'M4.

L'utilizzo degli Strumenti Aziendali deve sempre ispirarsi ai principi di massima diligenza, buona fede e correttezza; principi, questi, che devono costantemente uniformare e caratterizzare la condotta generale ed i singoli comportamenti di tutti i soggetti autorizzati all'uso dei predetti Strumenti.

Il Regolamento, pertanto, è finalizzato anche ad evitare che i Destinatari possano esporre sé stessi e/o l'M4 a sanzioni pecuniarie o penali, derivanti da un uso scorretto o illecito degli Strumenti Aziendali, nonché esporre M4 a una serie conseguenze pregiudizievoli, in relazione al suo patrimonio e/o alla sua immagine.

Ulteriore scopo del Regolamento è disciplinare le condizioni ed i limiti per il legittimo utilizzo delle postazioni di lavoro, dei servizi Internet e di ogni altro strumento e/o dispositivo informatico messo a disposizione dall'M4, al fine di diffondere una cultura della sicurezza informatica che concorra al conseguimento ed al mantenimento dei più alti livelli qualitativi dei servizi resi.

Scopo del Regolamento è anche quello di recepire e dare attuazione alle disposizioni normative e ai principi previsti dal Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (di seguito "**GDPR**"), nonché dei Provvedimenti emanati dal Garante per la protezione dei dati personali (di seguito "**Garante**") al fine di garantire la protezione dei dati personali trattati mediante tali strumenti, nonché la salvaguardia del patrimonio informativo aziendale, gli standard qualitativi dei servizi resi ed il *know-how* dell'M4 (costituito da dati, notizie ed informazioni di carattere strettamente riservato e confidenziale) da parte di coloro che agiscono nella struttura dell'M4 o che prestano la propria attività in favore della stessa anche al di fuori della sua struttura, indipendentemente dalla natura contrattuale del rapporto professionale in corso.

Al contrario, non rientra tra gli scopi del presente Regolamento il controllo a distanza e/o in forma occulta delle opinioni, abitudini e/o dell'attività dei suoi dipendenti, che rimangono strettamente vietati e non consentiti.

Pertanto, nel rispetto delle previsioni di cui agli artt. 4 e 8 della Legge 20 maggio 1970, n. 300 (di seguito "**Statuto dei Lavoratori**"), l'M4 intende anche disciplinare, con il Regolamento, le modalità di raccolta ed utilizzo delle informazioni e dei dati trattati tramite gli Strumenti Aziendali, informando circa l'esercizio dell'eventuale potere disciplinare dell'M4 nei confronti del Personale, qualora si verificasse ed accertasse - secondo le procedure e nel rispetto delle garanzie e tutele oggetto delle previsioni che seguono - un uso improprio e/o non autorizzato degli Strumenti Aziendali assegnati e/o in loro dotazione.

Il Regolamento e le previsioni ed indicazioni in esse contenute integrano dunque:

- a) l'apposita informativa resa dall'M4 ai sensi e per gli effetti dell'art. 4 dello Statuto dei Lavoratori, quanto al Personale, e in ogni caso dell'art. 13 del GDPR, in ordine alle modalità, finalità, procedure e relative tutele con riferimento al trattamento dei loro dati personali nel caso in cui si procedesse ad eventuali attività di controllo effettuate dalla stessa, anche attraverso strumenti di registrazione degli accessi e delle presenze (ad esempio *badge*) o mediante verifiche sull'utilizzo degli Strumenti Aziendali in loro dotazione per motivi professionali (ad esempio PC, *tablet*, *smartphone* aziendali), nonché della rete internet e della posta elettronica aziendale;
- b) le specifiche istruzioni già fornite al Personale nella lettera di designazione tra i "*Soggetti Autorizzati al*

Trattamento".

2. AMBITO DI APPLICAZIONE

Il Regolamento si riferisce ai trattamenti di Dati Personali effettuabili da M4 attraverso gli Strumenti Aziendali, per le finalità di seguito indicate:

- esecuzione della prestazione lavorativa da parte dei Lavoratori;
- eventuali procedure amministrative e procedimenti disciplinari, a seguito dei controlli posti in essere con le finalità e secondo le modalità specificate nel successivo paragrafo 5.2.10;

Il Regolamento si applica a tutti i soggetti che utilizzano gli Strumenti Aziendali, tra cui, a mero titolo esemplificativo e non esaustivo:

- a) lavoratori subordinati, nonché in distacco o in somministrazione, in ogni caso senza distinzione di durata, orario, ruolo, funzione e/o livello (ivi inclusi i dirigenti) e/o modalità di svolgimento della prestazione, compresi anche eventuali lavoratori in cd. "smart working" (di seguito, anche solo "il **Personale**")
- b) collaboratori, a prescindere dal rapporto contrattuale intrattenuti.

Tutti i soggetti sopra elencati saranno di seguito, congiuntamente, indicati come "**Personale**".

Il Regolamento costituisce anche espressione dei doveri di correttezza comportamentale e diligenza contrattuale e costituisce parte integrante del complessivo sistema normativo aziendale. In ogni caso, il Regolamento deve essere rispettato altresì da coloro che non siano Personale dell'M4.

Il presente Regolamento si applica altresì a qualunque soggetto che si trovi in possesso di specifiche credenziali di autenticazione per l'accesso alla rete informatica utilizzata dall'M4 o che comunque utilizzi, a qualsiasi titolo, anche in via temporanea, gli Strumenti Aziendali, in qualunque sede e/o ufficio, al fine di proteggere e mantenere riservati i dati trattati e di evitare che, attraverso l'eventuale utilizzo di tali strumenti l'M4 possa essere esposta a rischi.

I soggetti di cui sopra, unitamente al Personale, saranno di seguito congiuntamente indicati come "**Destinatari**".

3. RIFERIMENTI

- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 ("**GDPR**");
- Decreto Legislativo 101/2018, recante le disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016 (di seguito anche solo il "**Decreto**");
- Opinion 2/2017 del cd. "Article 29 Data Protection Working Party" dell'8 giugno 2017, "on data processing at work";
- Provvedimento del Garante del 1° marzo 2007, "Lavoro: le linee guida del Garante per posta elettronica e Internet", pubblicato in Gazzetta Ufficiale n. 58 del 10 marzo 2007 (di seguito anche solo il "**Provvedimento**");
- Provvedimento del Garante del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", pubblicato in Gazzetta Ufficiale n. 300 del 24 dicembre 2008 (di seguito anche solo il "**Provvedimento AdS**");
- Legge 20 maggio 1970, n. 300 "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale, nei luoghi di lavoro e norme sul collocamento" ("**Statuto dei Lavoratori**");
- CCNL applicabile e Codice di condotta dell'M4

4. DEFINIZIONI

Ferme le definizioni già previste nei paragrafi precedenti, le parole e le espressioni di seguito indicate hanno il seguente significato:

- **Amministratori di Sistema ("AdS")**: figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Vengono considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei Dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi;
- **Antivirus**: un software atto a rilevare ed eliminare virus informatici o altri programmi dannosi;

- **Back Up:** operazione tesa a creare una copia di sicurezza delle informazioni (dati o programmi);
- **Data Breach:** la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- **Dati Personali:** qualsiasi informazione riguardante una persona fisica identificata o identificabile: 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 uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- **DVD:** supporto di memorizzazione ottico delle informazioni;
- **File di Log:** file nel quale vengono registrate cronologicamente informazioni relative alle operazioni effettuate dagli utenti in un certo ambito (ad es. sistema, applicazioni, base dati); particolari file di log sono quelli relativi ai log di AdS che registrano attività di accesso ai sistemi eseguite dagli Amministratori di Sistema;
- **File Server:** area di archiviazione informatica presente su server aziendale;
- **Freeware:** software che viene distribuito in modo gratuito;
- **Funzione IT:** Unità organizzativa responsabile della implementazione di procedure e processi informatici;
- **Hardware:** qualunque parte fisica di un personal computer;
- **Hard Disk:** dispositivo di memoria di massa che utilizza uno o più dischi magnetici per l'archiviazione dei dati;
- **Interessati:** persone fisiche, identificate o identificabili, alle quali si riferiscono i Dati Personali
- **Laptop/PC:** personal computer portatile;
- **Malware:** software malevolo utilizzato per minacciare un sistema informatico e creare danni o chiedere riscatti;
- **Mailing list:** un sistema organizzato per la condivisione via mail di un argomento a più persone;
- **Network:** insieme di sistemi per l'elaborazione delle informazioni messi in comunicazione fra loro;
- **Normativa Applicabile:** il GDPR, gli artt. 4 e 8 dello Statuto dei Lavoratori, il CCNL di comparto, nonché il Provvedimento e tutti gli ulteriori provvedimenti e linee guida del Garante comunque applicabili;
- **Password:** parola segreta associata ad un User ID;
- **Password recovery:** attività di recupero di una password dimenticata o smarrita. L'attività di recupero consta nella generazione di nuova password (reset dell'esistente), operazione effettuata da un AdS o tramite una specifica funzionalità messa a disposizione all'utente da un sistema;
- **PdL:** Postazione di lavoro, sia fissa che mobile, ivi comprese le postazioni utilizzate per la distribuzione dei pasti in mensa;
- **Phishing:** attacco ingannevole, su Internet o mediante strumenti informatici (es. posta elettronica con l'invio di mail appositamente costruite per ingannare l'utente che le riceve), per indurre un utente a rivelare informazioni personali e/o aziendali (quali credenziali di accesso, codici, ecc.);
- **Responsabile del trattamento:** la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo, esterno all'M4, che tratta dati personali per conto della stessa, ai sensi dell'art. 28 GDPR;
- **Rete:** sistema di trasmissione dati che interconnette nodi indipendentemente dalla tecnologia utilizzata;
- **Rete M4:** rete aziendale di M4 in cui sono disponibili i servizi applicativi di backoffice, le risorse di rete per la condivisione di documenti, i servizi di autenticazione di dominio M4, etc.. e in cui sono attestate le PdL M4;
- **Screen Saver:** applicazione/funzione per computer che provoca lo standby del PC dopo un periodo programmato di inattività del mouse e della tastiera, impostabile attraverso un timer;
- **Server:** componente informatica che fornisce servizi ad altre componenti (tipicamente chiamate client) attraverso una rete;
- **Software:** programma o un insieme di programmi in grado di funzionare su un elaboratore;
- **Strumenti Aziendali:** Tutte le dotazioni hardware e software e le risorse informatiche aziendali dell'M4;
- **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 dei dati personali;
- **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 consulenza, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- **User ID:** codice identificativo associato ad una persona o ad un gruppo;

- **Virus:** un software che è in grado, una volta eseguito, di infettare dei file in modo da riprodursi facendo copie di sé stesso, potendo provocare danni sia al software che all'hardware;
- **Wireless:** sistema di comunicazione tra dispositivi elettronici, che non fanno uso di cavi.

5. DISPOSIZIONI IN MERITO AGLI OBBLIGHI DEI DESTINATARI CON RIGUARDO ALLE MODALITÀ D'USO DEGLI STRUMENTI AZIENDALI

Così come definito all'interno della "Procedura sulla protezione dei dati personali e sicurezza informatica" al fine di assicurare un adeguato livello di sicurezza delle informazioni, M4 ha predisposto sia una serie di misure e strumenti tecnici sia un insieme di regole e norme comportamentali che devono essere seguite ed osservate da tutti i Destinatari in relazione al trattamento di informazioni elettroniche e cartacee.

5.1 Norme di Comportamento

5.1.1 Comportamento professionale

M4 stabilisce le misure tecniche ed organizzative per assicurare la riservatezza e l'integrità delle informazioni e dei dati trattati con gli Strumenti Aziendali, in accordo con la Normativa Applicabile. È fatto assoluto divieto di cedere a terzi gli Strumenti Aziendali, anche in parte (ad esempio, SIM o auricolari, smartphone, PC portatili, tablet, PC fissi, etc..), o comunque di consentirne l'utilizzo da parte di terzi non autorizzati dall'M4. Tutti gli Strumenti Aziendali devono essere correttamente custoditi e mantenuti in buono stato dai Destinatari che devono contribuire, in rapporto ai propri ruoli, competenze e responsabilità, alla protezione dell'intero patrimonio dell'M4. È responsabilità dei Destinatari richiedere e consentire gli interventi manutentivi opportuni, segnalando tale necessità alla Funzione IT e segnalando altresì condizioni che impediscono l'esecuzione della manutenzione.

Costituisce regola generale che l'utilizzo degli Strumenti Aziendali deve essere limitato e strettamente vincolato all'esercizio di attività lavorative/professionali. Salve eventuali deroghe, che dovranno essere stabilite esclusivamente in forma scritta da M4, è proibito l'impiego degli stessi per scopi personali e/o di terzi e, in particolare, è vietato:

- utilizzare gli Strumenti Aziendali per uso personale;
- recare danni ai sistemi informativi, agli strumenti di supporto, ed in generale agli Strumenti Aziendali utilizzati dall'M4.

L'utilizzo di computer personali è permesso dietro autorizzazione scritta del Titolare con informativa resa alla Funzione IT, solo ed esclusivamente nei casi in cui non sia disponibile un computer aziendale con caratteristiche HW e SW adeguate a parere della Funzione IT e con i necessari programmi per lo svolgimento delle attività lavorative previste. La manutenzione del PC, in questo caso, è a completo carico dell'utente sia dal punto di vista hardware che software e durante l'utilizzo, dovranno sempre essere rispettate le norme contenute nel presente regolamento. In questo caso la Funzione IT provvederà alla configurazione necessaria del computer. Resta inteso che l'utilizzo della rete aziendale e l'accesso alla rete esterna tramite l'infrastruttura della Società, comporta necessariamente che il PC di proprietà del dipendente, sia dotato di software regolarmente licenziato e di antivirus ritenuto adeguato dalla Funzione IT e sarà cura dell'utente mantenere aggiornato il software antivirus.

5.1.2 Custodia, utilizzo e restituzione degli Strumenti Aziendali

I Destinatari sono responsabili della PdL e degli Strumenti Aziendali messi a loro disposizione dall'M4 e del loro utilizzo, avendo l'obbligo di custodire gli stessi con diligenza, segnalando eventuali furti, danneggiamenti o smarrimenti. Ogni utilizzo non inerente all'attività lavorativa/professionale può contribuire a generare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza informatica.

In assenza momentanea dei Destinatari, gli Strumenti Aziendali, con riferimento in particolare alla strumentazione mobile, devono essere custoditi in luoghi chiusi a chiave o, comunque, in luoghi sicuri contro il furto (es. in armadi chiusi).

Se un personal computer, o un qualsiasi altro Strumento Aziendale, viene portato fuori della sede aziendale (ad es. in caso di convegni, visite presso fornitori e/o clienti, etc.), devono essere prese tutte le precauzioni perché non venga smarrito, danneggiato o rubato. A tal proposito, i Destinatari devono prestare assoluta attenzione a non lasciare mai incustodita alcuna strumentazione ovvero conservarla in luoghi protetti.

I Destinatari che portano con sé gli Strumenti Aziendali, fuori dalla sede o dai locali dell'M4, devono assicurare la loro diligente conservazione e corretta gestione.

Qualora si dovesse verificare un furto o uno smarrimento, i Destinatari sono tenuti a comunicare immediatamente l'accaduto al Titolare, fornendo tutte le opportune informazioni e chiarimenti in merito affinché possa essere effettuata la denuncia.

E' vietato utilizzare sulla strumentazione informatica di M4 qualsiasi memoria di massa esterna (chiavette USB, hard disk, smartphone anche per ricarica tramite porta USB, etc.) non esplicitamente autorizzata dal Titolare.

E' vietato utilizzare servizi di web drive esterni alla rete M4 (quali a titolo esemplificativo e non esaustivo Wetransfer free) , non esplicitamente autorizzati dal Titolare, sulla strumentazione informatica di M4.

I Destinatari non devono modificare la configurazione hardware e/o software della postazione di lavoro (fissa e/o mobile), aggiungendo o rimuovendo componenti, rispetto allo standard definito e fornito dall'azienda. Qualora sia necessario, essi possono richiedere la modifica della propria configurazione hardware e/o software rivolgendosi all'AdS tramite il proprio diretto responsabile.

È assolutamente vietato installare modem, schede di rete, schede Adsl, schede wireless o qualsiasi altro dispositivo di connessione laddove non espressamente autorizzato. L'autorizzazione deve essere richiesta alla Funzione IT, tramite il proprio diretto responsabile, mediante invio di email IT@metro4milano.it.

Inoltre, i Destinatari, nella rete aziendale M4 sono tenuti a:

- utilizzare esclusivamente Hardware e Software forniti dall'M4;
- applicare le misure di sicurezza già previste nella lettera di designazione tra i "*Soggetti Autorizzati al Trattamento*" per garantire la protezione dei propri strumenti di lavoro e la sicurezza della propria postazione di lavoro;
- effettuare il log out dal proprio PC al termine della giornata lavorativa e spegnerlo, salvo diversa specifica indicazione data dalla Funzione IT ai fini della manutenzione della PdL;
- bloccare la sessione di lavoro del dispositivo quando lo stesso viene lasciato senza presidio (per i sistemi windows es. attraverso l'impostazione della modalità "*blocca computer*" tramite pressione contemporanea dei tasti Win+Lock);
- riportare ogni anomalia o malfunzionamento della postazione di lavoro (hardware, software, etc.) all'Ads.
- Infine, nella rete aziendale M4 le seguenti attività sono espressamente proibite:
- utilizzare od installare dispositivi hardware esterni per uso personale quali, a titolo esemplificativo ma non esaustivo, palmari, smartphone, agende elettroniche, unità USB, memorie flash, computer portatili, masterizzatori, Hard drive, lettori multimediali, non esplicitamente autorizzati dal Titolare, anche al solo fine di si ricarica energetica;
- Installare/copiare/effettuare download di programmi, virus, malware, macro, applet, controlli ActiveX, antivirus, antispam, firewall, od ogni altro dispositivo/software logico che causino, o possano causare, un cambiamento alle configurazioni dei sistemi aziendali o di terze parti;
- installare/effettuare download di software/applicativi non esplicitamente autorizzati dal Titolare;
- eliminare un programma o file installato legalmente in modo tale da impedire od ostacolare le normali operazioni, ivi inclusa la disattivazione dei sistemi di sicurezza;

I Destinatari, nell'utilizzo degli Strumenti Aziendali, devono tenere un comportamento improntato ai principi di correttezza e liceità. A tal riguardo, essi non dovranno effettuare nessun tipo di attività volta ad eludere o compromettere i meccanismi di protezione degli Strumenti Aziendali stessi, delle reti aziendali e/o di qualsiasi altro meccanismo di protezione comunque previsto. Il software realizzato da un lavoratore dipendente, nell'ambito del rapporto di lavoro e per finalità lavorative con strumenti dell'azienda, è di proprietà M4.

I Destinatari sono consapevoli e accettano di restituire la totalità degli Strumenti Aziendali che M4 abbia fornito o messo comunque a loro disposizione integri e in buono stato di conservazione, nel momento in cui cessa, a qualsiasi titolo e per qualunque motivo, il rapporto con M4, ovvero nel caso in cui non sussistano più le condizioni per le quali essi li avevano ricevuti, inclusi i casi di variazione di mansione e/o passaggio ad un altro

I Destinatari riconoscono e accettano che M4 potrà eseguire controlli sul contenuto degli Strumenti Aziendali restituiti nei termini previsti dal presente Regolamento, salvo che vi siano elementi che inducano M4 stessa a ritenere necessario un periodo di conservazione più lungo (ad esempio, per finalità di difesa di un diritto in sede giudiziaria), anche in seguito ad un'eventuale valutazione di impatto ai sensi e per gli effetti dell'art. 35 del GDPR. A riguardo, M4 ha individuato, per ciascuna categoria di dati, in relazione a ciascuna finalità, i relativi tempi di conservazione, che ha riportato in un apposito documento, di seguito, denominato " Policy di ritenzione dei dati personali" pubblicato nella bacheca aziendale.

5.1.3 Memorizzazione e protezione dei dati

L'integrità e la disponibilità delle informazioni e dei dati aziendali, ivi inclusi i Dati Personali di titolarità dell'M4, è garantita solo quando gli stessi sono memorizzati e trattati nell'ambito di sistemi all'uopo specificamente dedicati (ad esempio *File Server*), messi a disposizione dall'M4 ai vari Destinatari, gruppi di Destinatari, direzioni o unità organizzative.

I Destinatari sono tenuti a trasferire nella pertinente cartella di rete ("cartella di rete Z:\nome utente") tutti i dati eventualmente presenti nel personal computer messo a loro disposizione, con particolare riferimento ai dati considerati critici o di particolare rilevanza per M4 in ragione della loro specifica natura (dati confidenziali, segreti professionali/industriali) ovvero ai dati personali del cui trattamento M4 è titolare o responsabile ai sensi, rispettivamente, degli artt. 24 o 28 GDPR. Queste aree sui server aziendali devono essere utilizzate in maniera esclusiva e riservata e non dovranno eccedere la quota assegnata. Qualora l'utente necessiti di uno spazio maggiore potrà farne richiesta alla Funzione IT.

Costituisce buona regola la pulizia periodica della cartella di rete, da eseguirsi almeno ogni 3 (tre) mesi, con cancellazione dei file obsoleti o inutili. Particolare attenzione va prestata alla duplicazione dei dati, al fine di evitare un'archiviazione ridondante. Per facilitare dette operazioni di pulizia con cadenza almeno trimestrale la Funzione IT invierà specifico rapporto dell'analisi dei file duplicati per chiedere di effettuare una pulizia e riorganizzazione delle cartelle di rete.

I dati aziendali non devono essere estratti/copiati dai sistemi informativi aziendali, anche se utilizzando apposite funzionalità autorizzate secondo il profilo di abilitazione assegnato all'utente, in dispositivi che non siano Strumentazione Aziendale autorizzata dal Titolare.

I supporti di memoria rimovibili aziendali debitamente autorizzati (compact disk, hard disk USB, chiavette USB, ecc.) devono essere conservati in luoghi protetti (ad esempio, armadi e cassettiere chiusi a chiave). È sempre necessario verificare il contenuto informativo dei supporti di memoria, prima della loro consegna a terzi e prima della loro eliminazione/distruzione o sostituzione. In ogni caso, è necessario procedere alla cancellazione dei dati in essi contenuti quando non più necessari.

Se per errore o a causa di un malfunzionamento del sistema, o una problematica di configurazione o altro, i Destinatari dovessero entrare in possesso di informazioni confidenziali, o riservate, o che comunque non sono autorizzati a trattare (ad esempio e-mail inviata ad un destinatario errato, profilo di autorizzazione sugli applicativi non aggiornato a seguito cambio ufficio, etc.), saranno immediatamente tenuti a chiudere il programma di visualizzazione e a segnalare l'accaduto e chiedere istruzioni ad AdS, affinché siano prese le misure più opportune.

5.1.4 Gestione delle credenziali di accesso

L'accesso a tutti gli Strumenti Aziendali è sottoposto a procedure di identificazione personale (*log-in*) di tipo manuale, attraverso la digitazione di un identificativo univoco (User ID) e di una parola segreta (Password) necessari al riconoscimento della identità dei Destinatari da parte del sistema installato sugli Strumenti Aziendali e/o dell'applicazione in uso.

I Destinatari sono tenuti a conservare con la massima cura e segretezza tutte le Password di accesso alla rete, e ai sistemi: tali Password devono essere note solo ad essi e non possono essere condivise con altri soggetti. È comunque vietato ai Destinatari utilizzare credenziali di accesso diverse da quelle ricevute e successivamente aggiornate, in quanto strettamente personali ed assegnate in virtù del ruolo ricoperto, nonché alla luce del rapporto intercorrente con M4. I Destinatari sono inoltre tenuti a scollegarsi (*log-off*) al termine della sessione di lavoro e/o in caso di assenze dall'ufficio per un lungo periodo di tempo. In caso di prolungata assenza dei Destinatari o di un loro impedimento, il Titolare può chiedere alla Funzione IT di rendere disponibili e/o accessibili gli Strumenti Aziendali del Destinatario, informandone tempestivamente il Destinatario stesso.

Le credenziali di accesso ai sistemi M4 sono personali e non devono essere cedute. In ogni caso, i Destinatari devono seguire alcuni accorgimenti di estrema importanza nella scelta e nella gestione delle proprie credenziali di accesso. La Password ha una validità massima di 90 gg. Trascorso tale termine l'utente deve cambiarla. In particolare, per la gestione della password devono essere esplicitamente rispettate le seguenti regole.

La password o parola chiave:

- deve essere di almeno 12 caratteri;
- non deve contenere dettagli personali, anche se in forma parziale, come il proprio nome, la data di nascita, il numero di matricola, il Codice Fiscale e/o qualsiasi altro riferimento riconducibile ai Destinatari o alla loro storia personale;
- deve essere cambiata evitando di ripetere la medesima password con la sola variazione del carattere numerico (ad esempio qADNSgdfe3472!*1, qADNSgdfe3472!*2, ecc.);
- usare lettere minuscole, maiuscole, numeri, e un carattere speciale (es. ., ? \$! @ - > <), in ogni caso usare una combinazione di almeno tre tipologie di caratteri;

Inoltre:

- il Destinatario deve provvedere alla sostituzione della Password nel caso in cui essa venga rivelata o si sospetta che questo sia accaduto;
- i Destinatari sono responsabili di tutte le attività svolte attraverso l'uso del proprio identificativo personale (User ID); pertanto, non devono rivelare le proprie Password a nessuno e devono custodirle in modo appropriato. Allo scopo, le Password non devono mai essere trascritte su fogli, biglietti, post-it o su oggetti, soprattutto se posti nelle vicinanze del PC. Le Password inoltre non devono essere inserite in messaggi di posta elettronica e/o trasmesse attraverso qualsiasi altra forma di comunicazione elettronica in chiaro ovvero non crittografata, né possono essere salvate su strumenti e/o documenti informatici (ad es. file Word o Excel) che non siano protetti a loro volta da apposite credenziali.
- se lo User ID non viene utilizzato per più di sei mesi viene sospeso. Le credenziali di autenticazione sono disattivate se non usate da almeno 6 (sei) mesi e nel caso in cui il Dipendente dovesse perdere la qualità che gli consente l'accesso.
- nel caso in cui il Destinatario smarrisse la Password deve chiedere all'AdS di fornire una nuova password e provvedere ad inserirla e modificarla al primo accesso.

Per motivi di manutenzione o per nuove installazioni in cui si rendano necessarie configurazioni sul profilo utente, l'AdS può reimpostare la password del Destinatario, previo suo assenso, ed entrare con le sue credenziali. L'AdS notificherà al Destinatario immediatamente il termine della manutenzione ed il Destinatario dovrà cambiare prontamente la propria password.

Su motivata richiesta del Titolare, che provvederà ad avvisare il Destinatario, (es. accesso urgente a dati aziendali in caso di assenza del Destinatario) l'AdS può reimpostare la password del Destinatario, e consentire al Titolare l'accesso al profilo del Destinatario con le nuove credenziali. Al termine dell'attività il Titolare darà comunicazione al Destinatario di quanto avvenuto e il Destinatario dovrà cambiare la propria password.

5.1.5 Sottrazione alla vista delle informazioni su schermo

Gli Strumenti Aziendali e, in particolare, i personal computer non devono essere mai lasciati incustoditi. Anche in caso di breve assenza, e comunque ogniqualvolta ci si allontani dalla postazione di lavoro, il computer deve essere bloccato tramite le funzionalità offerte dal sistema operativo (es. attraverso l'impostazione della modalità "*blocca computer*" tramite pressione contemporanea dei tasti Ctrl+Alt+Canc e poi blocca o Win+Lock)).

È opportuno, inoltre, ogniqualvolta ci si allontani dalla postazione di lavoro, disconnettere gli applicativi in uso. In caso di inattività temporanea dei Destinatari per un periodo superiore ai 15 minuti, si attiverà automaticamente la funzionalità di “*salva schermo*” (*screen saver*), al fine di non consentire a terzi di visualizzare lo schermo del dispositivo lasciato incustodito e/o di accedere ai sistemi dello stesso.

Al termine della giornata lavorativa, i Destinatari sono tenuti a spegnere tutti gli Strumenti Aziendali utilizzati o, comunque, loro affidati, salvo diversa specifica indicazione data dalla Funzione IT ai fini della manutenzione della PdL.

5.1.6 Utilizzo dei sistemi di riproduzione

Gli Strumenti Aziendali devono essere utilizzati esclusivamente per motivi connessi all'esecuzione della prestazione lavorativa / professionale. La produzione di stampe o di copie di documenti cartacei e/o informatici o di duplicati di documenti informatici, specialmente riservati, deve essere il più possibile contenuta e limitata ai casi di effettiva necessità.

Durante la stampa, fotocopia, scansione di documenti, i Destinatari devono presidiare l'intero processo, al fine di impedire la volontaria o accidentale diffusione di Dati Personali o la perdita di riservatezza sulle informazioni contenute nei documenti stessi. Allo stesso scopo, è dovere dei Destinatari prelevare immediatamente i fogli riprodotti da stampanti e fotocopiatrici, e cancellare i file con dati personali e/o particolari dalle condivisioni accessibili a tutti i Destinatari autorizzati nella rete M4 (ad esempio sulla condivisione K:\Scambio).

5.2 Utilizzo degli Strumenti Aziendali e postazioni di lavoro

5.2.1 Strumenti di registrazione degli accessi

M4 fa uso di *badge*. I *badge* sono consegnati esclusivamente al Personale con lo scopo di registrarne l'accesso degli stessi ai luoghi di lavoro.

Gli strumenti di identificazione/autenticazione sono di stretta proprietà aziendale ed affidati direttamente ai singoli, che ne rispondono a titolo penale, disciplinare e patrimoniale. Essi non devono mai essere ceduti - ancorché temporaneamente ed anche per singolo utilizzo - a terzi, ivi compresi collaboratori, colleghi o persone di stretta fiducia. M4 utilizza altresì il sistema per registrare i log di accesso degli AdS.

5.2.2 Postazione di lavoro

Con riferimento alla propria postazione di lavoro, il Personale, al termine dell'orario di lavoro, deve in ogni caso:

- garantire che la postazione di lavoro (la scrivania fisica) sia priva di materiale o documenti contenenti dati personali che devono essere conservati in appositi cassetti e/o armadi debitamente chiusi o ad accesso limitato;
- se previsto, chiudere a chiave cassetti o di aree ad accesso limitato;
- raccogliere tutti i documenti stampati e i documenti non più necessari e provvedere alla loro definitiva eliminazione
- provvedere alla definitiva eliminazione dei documenti informatici non più necessari presenti nelle condivisioni di rete, nei dispositivi, nella postazione di lavoro; deve essere svuotato il cestino ad ogni cancellazione.

5.2.3 Internet

Al fine di garantire un appropriato utilizzo della rete Internet, tutti i Destinatari devono rispettare rigorosamente le seguenti regole:

- l'utilizzo del collegamento aziendale ad Internet per la navigazione sul web deve essere finalizzato a scopi esclusivamente lavorativi, ed in ogni caso nel rispetto del rapporto professionale con M4 e dei principi generali di liceità, responsabilità e correttezza della condotta;

- è consentita la navigazione su siti contenenti informazioni necessarie o utili all'attività lavorativa o, comunque, all'acquisizione di notizie utili alla propria formazione/informazione professionale;
- pur non essendo definito a priori un elenco di siti autorizzati, M4 può prevedere modalità di filtraggio, bloccando la navigazione su siti e/o categorie di siti i cui contenuti sono stati insindacabilmente ritenuti da M4 come estranei agli interessi ed alle attività di quest'ultima. In particolare M4 adotta uno specifico sistema di blocco su Firewall con filtro automatico (sistema di Web Filtering, Web Protection & Application Control), che previene l'accesso a determinati siti inseriti in black list classificate per reputazione negativa che vengono quotidianamente aggiornate. La rimozione del blocco potrà essere effettuata dalla Funzione IT su richiesta del singolo utente al suo responsabile previa autorizzazione del Titolare richiesta per iscritto. Nella richiesta sarà necessario indicare l'esatto indirizzo del sito internet da abilitare ed il motivo della richiesta.
- non è consentita la navigazione in siti e la memorizzazione di documenti informatici di natura oltraggiosa, violenta, pornografica e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica, posto che in ogni caso M4 ha previamente provveduto a predisporre appositi filtri che bloccano l'accesso ad una serie di siti ritenuti inidonei o pericolosi secondo le categorizzazioni del sistema di filtraggio;
- non è consentito scaricare e/o comunque installare software gratuiti (liberi, freeware, shareware) o in licenza d'uso anche se correttamente licenziati ma non di proprietà di M4, anche prelevati da siti Internet, e non autorizzati dal Titolare. L'autorizzazione deve essere richiesta mediante invio di email alla funzione IT che richiederà autorizzazione al Titolare per poi comunicarne esito al richiedente;
- è altresì proibito scaricare illecitamente video, testi, immagini, brani musicali, giochi e altri materiali protetti dal diritto d'autore e, comunque, violare in qualunque modo la Legge sul Diritto d'Autore e/o il Codice della Proprietà Industriale (con particolare, ma non esclusivo, riferimento al *know-how* dell'M4);
- non è permesso, per motivi non professionali, partecipare a forum, utilizzare chat line o bacheche elettroniche, social network, anche usando pseudonimi;
- tutti i file di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo antivirus; in caso di dubbio è sempre buona prassi coinvolgere la Funzione IT prima di aprire file di provenienza incerta e/o esterna;
- i Destinatari si impegnano a non interferire volontariamente con il buon funzionamento dei sistemi informatici e di rete di M4, avendo comunque la responsabilità di segnalare tempestivamente all'indirizzo e-mail dell'AdS, la presenza di attività sospette sui propri sistemi o sulla rete.

Una volta cessato il rapporto tra i Destinatari ed M4, a qualsiasi titolo e per qualunque ragione, copia del traffico internet sarà conservata sul server centrale e/o sui backup di M4, entro i termini previsti dalle Policy di ritenzione dei dati personali di M4, salvo che vi siano elementi che inducano M4 stessa a ritenere necessario un periodo di conservazione più lungo (ad esempio, per finalità di giustizia), anche in seguito ad un'eventuale valutazione di impatto ai sensi e per gli effetti dell'art. 35 del GDPR.

5.2.4 Intranet

L'accesso remoto alla rete aziendale deve avvenire esclusivamente attraverso l'uso di Strumenti Aziendali forniti da M4 (es. tramite VPN), attenendosi rigorosamente alle norme comportamentali espresse in questo Regolamento.

I Destinatari, se autorizzati dal proprio responsabile, possono collegarsi da remoto alla rete LAN aziendale mediante uso della VPN M4, che utilizza collegamenti che necessitano di autenticazione combinata tra server e firewall aziendale, con chiave cifrata a scadenza, a garanzia di accesso per i soli utenti autorizzati UserId presenti nel sistema. L'abilitazione e le credenziali di accesso vengono forniti dalla Funzione IT dietro richiesta scritta del Responsabile del Destinatario che ha necessità di collegamento da remoto, come a puro titolo di esempio per lo svolgimento delle proprie attività lavorative in modalità Smart Working.

Il software dedicato, per l'accesso alla VPN M4, deve essere installato esclusivamente dalla Funzione IT che ne gestisce la configurazione. Il software utilizza dei certificati digitali che hanno pertanto una scadenza, al termine del quale, per aumentare il livello di sicurezza nelle connessioni viene rinnovato dai sistemi. Particolare cautela deve essere posta, inoltre, nell'utilizzo di reti Wi-Fi pubbliche e/o gratuite per accedere alla rete M4 e al servizio di posta elettronica aziendale, dal momento che nell'accedere a tali servizi devono essere inserite le credenziali e che queste ultime potrebbero essere facilmente carpite.). In particolare si richiede ai Destinatari di non far

uso per quanto possibile di reti pubbliche ed utilizzare preferibilmente la funzione hot spot dello smartphone aziendale.

5.2.5 Posta elettronica aziendale

La posta elettronica, messa a disposizione da M4 a favore dei Destinatari all'uopo autorizzati, rappresenta uno strumento di esclusiva proprietà aziendale per lo svolgimento di attività lavorative/ professionali.

L'utenza di posta elettronica aziendale è strettamente personale ed è pertanto responsabilità di ciascun utente garantire la riservatezza delle credenziali di accesso al servizio nonché il corretto utilizzo dello stesso. Inoltre, possono essere resi disponibili, sulla base di necessità operative/organizzative, indirizzi di posta elettronica per le strutture aziendali, ad uso comune, condivisi tra i soggetti assegnati al medesimo servizio (ad esempio, amministrazione@metro4milano.it e segreteria@metro4milano.it). Il Responsabile del Servizio richiedente dovrà comunicare alla Funzione IT i nominativi delle persone autorizzate all'utilizzo della casella di posta al fine di potergli concedere l'accesso. Anche tali indirizzi di posta elettronica sono di esclusiva proprietà aziendale e i Destinatari all'uopo autorizzati condivideranno la responsabilità del loro utilizzo.

Per una corretta fruizione del servizio di posta elettronica aziendale, ivi compresa la PEC aziendale per i Settori di competenza, che tuteli i Destinatari e l'M4, devono essere rispettate le seguenti regole:

- è necessario fare attenzione alla posta ricevuta. Nel caso di mittenti sconosciuti o messaggi insoliti, di dubbia autenticità o provenienza e/o con contenuti non attinenti al lavoro svolto, per non correre il rischio di essere infettati da virus e/o malware e/o di essere vittima di Phishing, è necessario verificare il sorgente/intestazione/header del messaggio ricevuto e in caso di dubbio occorrerà contattare immediatamente il personale della Funzione IT. A seguito verifica con individuazione di possibili minacce si deve procedere con la cancellazione dei messaggi senza aprirli. In particolare, non dovranno essere aperti documenti di cui non si è certi della provenienza e documenti con estensioni diverse da quelle comunemente utilizzate e autorizzate (.doc, .xls, .ppt, .pdf) e/o con nomi "sospetti" e/o "anomali". Qualora, in allegato ad un'e-mail, vi fossero file sospetti o anomali (estensione .exe anche contenuti in file .zip/7z/Rar) è necessario accertarsi preventivamente del loro contenuto, verificando il mittente del messaggio e contattando il mittente medesimo per assicurarsi della trasmissione o per informarlo di una possibile problematica sui propri sistemi informatici (es. la presenza di malware che effettua invii a sua insaputa). Non bisogna pigiare link di provenienza dubbia o incerta senza averli verificati in quanto con il click del mouse su un collegamento malevolo all'interno di una mail, è possibile infettare le postazioni di lavoro in modo irreparabile. Per precauzione, contattare immediatamente la Funzione IT. In ogni caso è obbligatorio controllare tutti i file in allegato prima del loro utilizzo e non eseguire download di file eseguibili. Il Destinatario deve prestare particolare attenzione a file di tipo archivio compresso (.zip, .rar, .tar, .tar.gz, .gz, etc...) che dovessero essere allegati a mail in quanto possono contenere file eseguibili dannosi di tipo malware. In caso di dubbi, contattare immediatamente la Funzione IT;
- nel caso si riscontrassero chiari casi di tentativi di *Phishing* (tipo di frode ideata allo scopo di carpire importanti dati personali, ad esempio numeri di carta di credito, password, dati relativi al proprio account, ecc.), marcare i mittenti come bloccati in Posta Indesiderata, cancellare i messaggi senza aprirli e rendere immediata segnalazione al Responsabile della Funzione IT;
- accertarsi che gli eventuali allegati dei propri messaggi non eccedano la dimensione massima prevista per l'invio del sistema (30Mb) o per il destinatario;
- inviare allegati solo nei formati più usati: ad es. *.txt, *.rtf, *.docx, *.pptx, *.xlsx, *.pdf, *.gif, *.tif*, jpg;
- non è consentito inviare o memorizzare messaggi di natura oltraggiosa, violenta, volgare e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, forum, social network o mailing-list, salvo diversa ed esplicita autorizzazione da richiedere al proprio responsabile informando la Funzione IT all'indirizzo IT@metro4milano.it. L'iscrizione ad una mailing list o a servizi simili (chat, forum, social network, ecc.) è consentita solo se funzionale all'attività aziendale e previa autorizzazione del proprio responsabile;

- non è, altresì, consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per inviare messaggi di tipo umanitario, sociale o di solidarietà, salvo diversa ed esplicita autorizzazione rilasciata dal proprio responsabile;
- non è consentito utilizzare la posta elettronica per finalità che esulano dall'espletamento delle mansioni affidate a ciascun Destinatario;
- non è consentito creare, archiviare o spedire messaggi pubblicitari o promozionali in nessun modo connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto;
- non è consentito inviare messaggi in risposta a richieste di adesione a programmi di catene di e-mail, indipendentemente dalle finalità per M4;
- la posta elettronica non deve essere utilizzata per ricevere, memorizzare o spedire materiale che violi le norme sul diritto d'autore o proprietà industriale (copyright, marchi, ecc.);
- ogni e-mail inviata all'esterno deve contenere, come nota finale allegata in automatico, un'adeguata informativa relativa alle informazioni confidenziali. Si consiglia di utilizzare la seguente:
 - *"Questo messaggio (compreso ogni eventuale allegato) è riservato ad uso esclusivo dell'individuo o dell'ente o soggetto giuridico cui è indirizzato e può contenere informazioni che sono da intendersi come riservate e non destinate a pubblica divulgazione e soggette a tutela legale. Se non siete i destinatari di questo messaggio non dovete farne uso, diffonderlo o estrarne copia, in qualunque forma, né fare affidamento sul suo contenuto. Nel caso in cui Le fosse giunta per errore, La preghiamo di (i) comunicarcelo e (ii) provvedere alla sua distruzione immediata. Questo indirizzo di posta elettronica non è un indirizzo di posta privato e perciò il suo utilizzo è soggetto a regolamentazione."*
- è opportuno inserire la propria firma in calce alle e-mail, riportando la direzione e l'unità di appartenenza, secondo le istruzioni sotto:

(Titolo) Nome Cognome

(Ruolo) Settore di appartenenza

Telefono fisso

Telefono mobile



Piazza Castello 3 - 20121 Milano

tel. 02 72629501 - www.metro4milano.it

- quando possibile, inviare gli allegati ai messaggi rivolti a destinatari esterni all'M4 in un formato compresso (*.zip, *.7z *.rar), al fine di ottenere un messaggio di dimensioni più contenute possibile, riducendo così il rischio di un mancato recapito a causa delle sue dimensioni eccessive;
- sempre per ragioni di contenimento della dimensione dei messaggi, è fortemente sconsigliato inserire immagini o altri file multimediali nel loro corpo o nella "firma" (con eccezione fatta per quanto indicato al capoverso precedente sulla firma);
- qualora si renda necessario inviare immagini per motivi d'ufficio (es. per inviare la cattura dello schermo di una maschera di un gestionale al fine di documentare una anomalia/errore di un servizio applicativo/programma software) si devono rendere inintelligibili eventuali i dati personali presenti (es. utilizzando strumenti grafici a bordo delle PdL come paint o gimp);
- i Destinatari sono tenuti a mantenere in ordine la propria casella di posta elettronica, cancellando documenti inutili ed e-mail non necessarie, in modo tale da razionalizzare l'impiego delle risorse informatiche e tecnologiche disponibili;
- è opportuno scrivere i propri messaggi di posta elettronica in un formato congruente con il programma di posta del destinatario (normalmente il formato di puro testo viene sempre accettato);
- è definito un limite massimo delle dimensioni di una casella postale di 50 Gb per ciascun utente autorizzato;
- raggiunta la soglia di avviso prima della dimensione massima, all'utente sarà notificato dal sistema di posta elettronica il superamento di tale soglia. Superato il limite massimo, l'invio di nuovi messaggi sarà automaticamente inibito e l'utente dovrà necessariamente procedere alle operazioni previste per ripristinare la funzionalità della propria casella postale (cancellazione e/o archiviazione della posta), autonomamente;

E' fatto espresso divieto di usare la casella di posta elettronica aziendale per ragioni e/o finalità personali e di inoltrare, in qualunque modo, verso eventuali strumenti di web mail personali, messaggi ricevuti sulla casella di posta elettronica aziendale e/o dati, documenti e/o informazioni di M4

Infine, si informa che in alcuni casi particolari, su esplicita richiesta delle Autorità competenti (Guardia di Finanza, Autorità Giudiziaria, ecc.), le e-mail memorizzate nei server di M4 potrebbero essere eventualmente rese note e consegnate alle stesse.

Nei casi di assenza programmata, il Personale dovrà utilizzare il sistema di risposta automatica disponibile (attualmente sia da client di posta installato sul PC sia tramite webmail) della posta elettronica aziendale indicando almeno la data di inizio del periodo di assenza, la data di ripresa del servizio e, al fine di garantire la continuità del servizio, ove possibile, dovrà indicare il nominativo di un altro utente a cui potrà essere inviata, in copia conoscenza, la propria corrispondenza elettronica. In caso di prolungata assenza o in situazioni di emergenza, i Destinatari potranno attivare tale dispositivo di risposta automatica in riferimento ai rispettivi indirizzi di posta elettronica aziendale.

In previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, il Personale potrà delegare un'altra persona (fiduciario) approvato dal Responsabile, a verificare il contenuto dei messaggi e ad inoltrare ad M4 quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.

In ogni caso, al fine di assicurare la disponibilità per M4 del contenuto della casella di posta elettronica aziendale, in caso di improvvisa o prolungata assenza dei Destinatari o di un loro impedimento, l'accesso alla predetta casella di posta elettronica aziendale potrà essere effettuato dall'AdS su esplicita e motivata richiesta scritta del Titolare. Sarà cura degli Ads realizzare dei *report* di tali attività al fine di informare il Destinatario interessato alla prima occasione utile.

Nel caso di cessazione del rapporto di lavoro (subordinato/ di collaborazione o somministrazione, ecc.), al fine di consentire la continuità lavorativa M4, previa immediata disattivazione dell'account di posta elettronica aziendale, potrà su richiesta del responsabile del Destinatario attivare un sistema di risposta automatica che informi i mittenti delle e-mail della disattivazione dell'*account* di posta elettronica aziendale /o della cessazione del rapporto di lavoro, invitandoli a contattare altro dipendente/funzione aziendale.

Una volta disattivato l'account di posta elettronica, copia dei messaggi di posta elettronica sarà conservata sul server centrale e/o sui *backup* dell'M4, entro i termini previsti dal presente Regolamento e/o della "Policy di ritenzione dei dati personali", salvo che vi siano elementi che inducano M4 stessa a ritenere necessario un periodo di conservazione più lungo (ad esempio, per finalità di difesa di un diritto in sede giudiziaria), anche in seguito ad un'eventuale valutazione di impatto ai sensi e per gli effetti dell'art. 35 del GDPR.

5.2.6 Software

È opportuno, per garantire la sicurezza del Software messo a disposizione da M4, che i Destinatari rispettino le seguenti regole:

- M4 acquista le licenze d'uso dei Software per gli Strumenti Aziendali da varie società esterne, pertanto è soggetta a limitazioni nell'utilizzo di tali programmi e, a meno di una specifica autorizzazione concessa dallo sviluppatore del software, non ha il diritto, e con essa i Destinatari, di riprodurlo, a meno di ragioni di salvataggio (copie di back-up opportunamente documentate);
- per quel che riguarda le applicazioni (client/server, web based e genericamente in rete), i Destinatari sono tenuti a utilizzare i Software loro concessi in uso solo entro i limiti specificati nei relativi contratti di licenza;
- non è consentito riprodurre, adattare, trasformare, distribuire Software in licenza d'uso aziendale;
- non sono consentiti il dispiegamento, l'installazione e l'uso di qualsiasi tipo di software anche libero non preventivamente autorizzato dal Titolare e previa informazione alla Funzione IT;

- come stabilito dalla Legge sul Diritto d'Autore, è assolutamente vietata la duplicazione illegale dei software; coloro che violino detta disposizione sono responsabili sia civilmente sia penalmente e quindi possono essere condannati al pagamento dei danni e anche alla reclusione. I Destinatari che effettuano, acquisiscono o usano copie non autorizzate del Software subiranno le relative sanzioni disciplinari previste, ove applicabili.

È inoltre assolutamente vietato utilizzare e/o installare software atti ad intercettare, falsificare, alterare il contenuto di documenti informatici (a titolo esemplificativo: programmi di *password recovery*, *password cracking*, *sniffing*, *spoofing*, *keylogger*, ecc.).

L'aggiornamento del sistema operativo avviene in modo automatico attraverso la rete aziendale. Qualora il computer resti scollegato dalla rete aziendale sarà a cura del Destinatario provvedere all'aggiornamento immediatamente qualora il sistema ne faccia richiesta. La Funzione IT fornisce supporto ai Destinatari nell'effettuare tale aggiornamento.

Nel caso in cui i Destinatari vengano a conoscenza di una qualsiasi vulnerabilità derivante da difetti di configurazione o difetti intrinseci ai programmi e/o ai sistemi e/o alla rete e alle sue configurazioni, essi dovranno darne tempestivamente comunicazione alla Funzione IT.

Esclusivamente su chiamata dell'utente la Funzione IT potrà effettuare interventi da remoto mediante l'utilizzo di un apposito software installato sul PC dei Destinatari previa notifica preventiva della data dell'accesso e della durata dello stesso al fine della risoluzione del malfunzionamento lamentato.

Ai fini della manutenzione del sistema viene creato su ogni PC un profilo Utente "Administrator" con relativa password ad uso esclusivo dell'Ads. L'utilizzo della password del profilo utente "Administrator" da parte dell'AdS viene tracciato.

È fatto in ogni caso specifico divieto di disinstallare il Software o di modificare gli standard di configurazione dei Software installati sul proprio PC o cancellare o modificare il profilo "Administrator" creato per la manutenzione.

5.2.7 Antivirus

Ogni personal computer viene corredato di software antivirus standard aziendale, adeguatamente configurato ed aggiornato. Le politiche di sicurezza M4 prevedono l'utilizzo in tutti i computer di uno stesso software antivirus di classe enterprise (in uso Trend Micro Worry-Free Business Security Services®), con distribuzione e gestione centralizzata, che viene aggiornato automaticamente. Non è ammesso l'utilizzo di sistemi antivirus diversi, se non espressamente autorizzati per iscritto, dalla Funzione IT.

È vietato disattivare il software antivirus o modificarne la configurazione. È doveroso collegarsi periodicamente alla rete interna per consentire il caricamento dell'aggiornamento dell'antivirus e seguire le istruzioni eventualmente impartite dalla Funzione IT. E' responsabilità di ciascun Destinatario effettuare prontamente l'aggiornamento del software antivirus, qualora il sistema lo segnali.

I Destinatari che abbiano ricevuto in dotazione Strumenti Aziendali non possono installare né ulteriori software antivirus, né altri diversi da quelli standard aziendali. L'AdS, ai fini di manutenzione e di risoluzione di incidenti informatici sulle PdL, può installare strumenti di identificazione, di rimozione e motori antivirus ulteriori in piena autonomia.

I Destinatari devono tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale da parte di virus o ogni altro software aggressivo o malware (ad esempio non aprire mail o relativi allegati sospetti, non navigare su siti non professionali o di indubbia integrità, ecc.).

Prima di caricare un qualunque tipo di dato o programma da un supporto esterno aziendale (floppy disk, hard disk USB, pen flash USB, cassette magnetiche, CD-ROM, ecc.) i Destinatari devono essere stati preventivamente autorizzati dalla Funzione IT e procedere alla scansione del supporto utilizzando l'antivirus messo a disposizione da M4. Nel caso venga rilevato un virus non eliminabile dal software antivirus, i Destinatari non devono utilizzare il dispositivo infetto.

Nel caso in cui il software antivirus rilevi la presenza di un virus (anche che non sia riuscito ad eliminare), i

Destinatari devono immediatamente sospendere ogni elaborazione in corso, senza spegnere il computer e segnalare l'accaduto alla Funzione IT.

Il Destinatario deve verificare che l'antivirus sia presente ed aggiornato sul dispositivo che sta utilizzando e in caso contrario deve segnalare l'accaduto alla funzione IT.

5.2.8 Telefoni / tablet

I telefoni, fissi e/o *mobile*, e i *tablet* sono eventualmente affidati ai Destinatari al solo fine di rendere la prestazione lavorativa e devono essere utilizzati secondo le modalità indicate nel presente paragrafo. E' fatto quindi divieto di un cd. "*uso promiscuo*" e, pertanto, l'utilizzo di queste apparecchiature ai fini privati è consentito solo in caso di comprovata necessità o urgenza. Nel caso di uso personale di Strumenti Aziendali il Dipendente sarà ritenuto esclusivo responsabile per ogni eventuale danno che dovesse derivare da detto utilizzo privato.

Inoltre, con particolare riferimento agli eventuali telefoni *mobile* / *tablet*, nell'ambito del contratto aziendale, è altresì fatta espressa indicazione di:

- evitare di chiamare numeri a pagamento, salva preventiva autorizzazione scritta del proprio responsabile ;
- proteggere tutti i dati presenti nel dispositivo, anche mediante cd. "*pin code*" (o strumenti analoghi), sistemi di blocco automatico dello schermo e cifratura;
- evitare di scaricare e/o installare applicazioni non preventivamente richieste dal diretto superiore e autorizzate dal Titolare alla Funzione IT o che, comunque, che non siano coerenti con l'esclusivo utilizzo lavorativo del telefono;

In ogni caso, qualora la sicurezza dei dati presenti sul telefono *mobile* / *tablet* sia insindacabilmente ritenuta a rischio da parte di M4 (e.g. in caso di smarrimento, e/o alla luce di *bug* e/o notizie di possibili *breach* ecc.), quest'ultima potrà intervenire, anche da remoto, sugli Strumenti Aziendali previa richiesta di autorizzazione al Titolare per iscritto.

5.2.9 Controlli da parte dell'M4

In relazione agli Strumenti Aziendali, M4 si riserva la facoltà di effettuare controlli saltuari e occasionali per verificare l'integrità del sistema informatico, il loro uso equilibrato e conforme all'attività ed alle politiche aziendali degli Strumenti Aziendali e per l'ordinaria manutenzione degli stessi, nonché per tutte le finalità connesse al rapporto di lavoro, riservandosi, in ogni caso, di accertare e segnalare tempestivamente eventuali abusi/violazioni commessi dai Destinatari.

In ogni caso viene garantito ai Destinatari il rispetto dei principi di liceità, pertinenza e non eccedenza previsti dalla Normativa Applicabile, nell'effettuazione di eventuali controlli, nonché il rispetto del divieto dei controlli a distanza dei lavoratori dipendenti.

Per le suddette ragioni, M4 si riserva di monitorare le reti e tutti gli altri Strumenti Aziendali, in particolare, nelle seguenti situazioni:

- necessità di effettuare verifiche sulla funzionalità e sulla sicurezza dei sistemi;
- constatazione di utilizzo indebito della posta elettronica, della rete Internet, della fonia fissa e mobile;
- necessità di effettuare verifiche tese alla protezione del patrimonio dell'M4;
- presenza di casi di abusi da parte di singoli o reiterati;
- presenza di indizi relativi alla fuga di informazioni riservate o confidenziali.

Controlli periodici possono essere effettuati:

- sul volume dei messaggi scambiati;
- sul formato e la dimensione dei file allegati;
- sulla durata dei collegamenti ad Internet (globale, per funzione, per gruppi o tipologia di utenti);
- sui siti visitati più frequentemente (globale, per funzione, per gruppi o tipologia di utenti);
- sulle informazioni raccolte dai dispositivi di sicurezza (Firewall, Antivirus, IDS, IPS, proxy, ecc.).

Le informazioni relative ai file *log* verranno trattate esclusivamente dall'AdS per verifiche periodiche o per la risoluzione di anomalie o problematiche o su richiesta del Titolare.

Le modalità con cui verranno effettuati i controlli saranno le seguenti:

- i controlli, ove possibile, verranno effettuati preventivamente su informazioni appartenenti a gruppi collettivi di Destinatari, su dati aggregati tramite l'analisi di statistiche anche generali;
- successivamente, verranno inoltrati avvisi collettivi di diffida al compimento di operazioni non consentite o, a seconda della gravità, verranno prese misure di tipo individuale, specialmente in caso di abuso e/o anomalie reiterate;
- i dati relativi ai file log di navigazione verranno conservati per un periodo di n. 12 mesi funzionalmente alla capienza dei server (Policy di ritenzione dei dati personali);
- nei casi in cui si debba far fronte a particolari esigenze tecniche o di sicurezza oppure si debbano utilizzare i dati registrati con riferimento all'esercizio o alla difesa di un diritto in sede giudiziaria (azioni da parte di terzi verso l'M4 o viceversa, o in caso di verifiche relative ad un presunto comportamento illecito), oppure si ottemperi all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria, tale periodo verrà prolungato secondo le necessità del caso e nel pieno rispetto delle finalità descritte;
- in ogni caso verranno esclusi controlli prolungati, costanti o indiscriminati o comunque preordinati al controllo a distanza dei lavoratori.

A tal riguardo si precisa che:

- in ogni caso non si fa luogo alla lettura e alla registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail (il server di posta memorizza i messaggi finché il Destinatario li cancella o li archivia offline su file locali alla postazione di lavoro), ivi inclusi i salvataggi periodici dei dati (c.d. "back up");
- inoltre, non si procede alla riproduzione o memorizzazione sistematica delle pagine web visualizzate dall'Utente, né alla lettura e alla registrazione dei caratteri inseriti tramite tastiera o analogo dispositivo né all'analisi occulta dei computer portatili affidati in uso.

L'AdS può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericoloso per la sicurezza, sia sul PC dei Destinatari che sulle unità di rete, o delegare la rimozione.

L'effettuazione di tali controlli, che non ha lo scopo di monitorare l'attività dei Destinatari, bensì di verificare la sicurezza del sistema e di effettuare la manutenzione, avverrà nel pieno rispetto della Normativa applicabile.

Con particolare riferimento all'utilizzo dei telefoni aziendali, l'M4 potrà effettuare verifiche periodiche volte a verificare la coerenza dei costi derivanti dalle utenze telefoniche associate con i suddetti apparecchi, nel pieno rispetto della Normativa applicabile. A tal proposito verranno segnalati ai Destinatari eventuali discrepanze o problemi che dovessero essere riscontrati nel corso di tali controlli.

Di tali controlli e del relativo trattamento dati è stata fornita informativa ai Destinatari con il presente Regolamento, anche ai sensi dell'art. 13 del GDPR. L'eventuale conservazione di tali dati avverrà per il tempo strettamente limitato al perseguimento lecito di finalità organizzative, produttive e di sicurezza.

Il mancato rispetto o la violazione delle regole contenute nel Regolamento è perseguibile con provvedimenti disciplinari previsti dal CCNL, ed altresì con le azioni civili e penali previste dalle leggi vigenti, qualora si verifichino gli estremi per la sussistenza della responsabilità civile o penale.

I sistemi preposti alla gestione di Internet, della posta elettronica e della rete interna aziendale registrano, su appositi file di sistema detti file di LOG, una serie di informazioni aggregate.

Ove possibile, i dati sono acquisiti in modalità anonima e quindi non riconducibili direttamente all'identità dei singoli Destinatari che li hanno generati. Tali dati saranno archiviati, con le opportune misure di sicurezza e riservatezza, ed eventualmente controllati nei limiti sanciti dalla normativa vigente e dal presente Regolamento nonché dalla "Policy di ritenzione dei dati personali", fatte salve eventuali esplicite richieste delle Autorità competenti e/o salvo che vi siano elementi che inducano M4 stessa a ritenere necessario un periodo

di conservazione più lungo (ad esempio, per finalità di giustizia), anche in seguito ad un'eventuale valutazione di impatto ai sensi e per gli effetti dell'art. 35 del GDPR.

5.2.10 Conservazione

I file di LOG contengono le informazioni relative ad almeno gli ultimi 180 giorni. I dati contenuti nei LOG possono essere trattati in via eccezionale e tassativamente nelle seguenti ipotesi:

- per corrispondere ad eventuali richieste della polizia giudiziaria e/o dell'autorità giudiziaria;
- allorquando sia necessario un intervento – espressamente richiesto dall'utente, dal Responsabile dell'Ufficio competente, dal Titolare – volto al recupero di dati contenuti in file o e-mail accidentalmente andati persi.

Quotidianamente vengono salvati, su supporto esterno Nas, tutti i file e dati relativi a cartelle di rete e database.

Il contenuto dei dispositivi di memorizzazione degli Strumenti Aziendali, delle cartelle dei *File Server*, degli *account* di posta elettronica aziendale saranno conservati sul server centrale e/o sui *backup* di M4 secondo la politica di backup, fatte salve eventuali esplicite richieste delle Autorità competenti e/o salvo che vi siano elementi che inducano M4 stessa a ritenere necessario un periodo di conservazione più lungo (ad esempio, per finalità di giustizia), anche in seguito ad un'eventuale valutazione di impatto ai sensi e per gli effetti dell'art. 35 del GDPR.

Il traffico Internet sarà cancellato da M4 periodicamente, fatte salve eventuali esplicite richieste delle Autorità competenti e/o salvo che vi siano elementi che inducano M4 stessa a ritenere necessario un periodo di conservazione più lungo (ad esempio, per finalità di giustizia), anche in seguito ad un'eventuale valutazione di impatto ai sensi e per gli effetti dell'art. 35 del GDPR.

5.2.11 Istruzioni in caso di cessazione del rapporto di lavoro o di collaborazione

Fermo quanto previsto dai paragrafi precedenti, in caso di cessazione del rapporto di lavoro o di collaborazione e in tutti i casi in cui ciò sia richiesto da M4 (quali ad esempio il venir meno delle ragioni di servizio che avevano determinato l'assegnazione, la sua sostituzione con altro Strumento Aziendale), gli Strumenti Aziendali dovranno essere restituiti senza cancellare alcun dato aziendale ivi memorizzato, e mantenendo il dato leggibile (i file non devono essere crittografati) da intendersi sin d'ora di esclusiva proprietà dell'M4, avendo cura i Destinatari di eliminare preventivamente soltanto tutti i propri eventuali dati personali riferiti o riferibili al Destinatario medesimo, nonché le eventuali informazioni e comunicazioni, personali non attinenti l'attività lavorativa svolta che gli stessi abbiano eventualmente archiviato negli Strumenti Aziendali in dotazione, in tal caso violando quanto previsto dal presente Regolamento.

Più in dettaglio, nell'ipotesi di cui al precedente paragrafo, i dati custoditi dai Destinatari afferenti gli Strumenti Aziendali dovranno, comunque, essere restituiti integralmente ad M4, secondo quanto previsto dalla lettera di nomina a "*Referente Privacy*" e/o di designazione tra i "*Soggetti Autorizzati al Trattamento*" con espresso divieto di conservarli, duplicarli, comunicarli o diffonderli. Quando il rapporto di lavoro o collaborazione con il Personale venga a cessare, i dati, le informazioni, i *file* e archivi di lavoro inerenti l'attività lavorativa / professionale svolta dallo stesso, inclusi quelli riportati o allegati nelle *e-mail*, devono essere senz'altro restituiti ad M4, la quale è tenuta a conservare questi dati ed informazioni solo a fini inerenti la gestione aziendale senza duplicare, comunicare o diffondere alcun dato personale.

5.2.12 Violazioni e sanzioni

Le istruzioni contenute nel presente Regolamento hanno valore di normativa aziendale e la loro violazione può comportare l'applicazione di sanzioni disciplinari previste dal CCNL.

La non ottemperanza delle suddette disposizioni potrà determinare l'applicazione da parte di M4 di restrizioni considerate appropriate, nonché l'applicazione da parte della stessa:

- di provvedimenti disciplinari a carico del Personale, previsti dal regolamento aziendale e dal CCNL;
- della eventuale risoluzione del contratto e delle azioni civili e penali stabilite dalla legge, nei confronti dei collaboratori.

5.2.13 Osservanza delle disposizioni in materia di protezione dei dati personali

È, in ogni caso, obbligatorio attenersi alle disposizioni in materia di protezione dei dati personali e di misure minime di sicurezza, nonché alle istruzioni fornite da M4.

5.2.14 Entrata in vigore del Regolamento e pubblicità

Il presente Regolamento entrerà in vigore con la sua approvazione da parte del Consiglio di Amministrazione e pubblicazione sul sito istituzionale della società.

5.2.15 Modifiche e aggiornamenti

In caso di modifiche successive ritenute necessarie/opportune gli uffici emittenti provvederanno ad aggiornare il documento e riattivare in coordinamento con l'Ufficio Legale l'iter di approvazione da parte del Consiglio di Amministrazione. Gli uffici emittenti hanno altresì il compito di monitorare nel tempo l'adeguatezza ed effettiva applicazione del presente Regolamento.

5.2.16 Diffusione

La Segreteria Societaria è responsabile di archiviare in apposite cartelle di rete aziendali e diffondere internamente (in apposita sezione del sito web aziendale e via mail ai Soggetti Rilevanti preventivamente identificati) la procedura ed ogni sua successiva modifica/aggiornamento a seguito di approvazione da parte del Consiglio di Amministrazione.