REGOLAMENTO PER LA GESTIONE DEL PATRIMONIO INFORMATIVO AZIENDALE - Immedia SpA

Conforme alla norma UNI EN ISO 9001:2015
Conforme alla norma UNI EN ISO 14001:2004
Conforme alla norma UNI EN ISO 27001:2008
Conforme al Modello previsto dal D.Lgs 231/2001
Conforme al D.Lgs 196/2003 novellato dal D.Lgs. 101/2018
Conforme al GDPR 2016/679

Sommario

PREMESSA 3
1) AFFIDAMENTO APPARATI TECNOLOGICI NECESSARI ALLO SVOLGIMENTO DEL LAVORO 3
2) MODALITA' DI UTILIZZO DEL PERSONAL COMPUTER 3
3) MODALITA' UTILIZZO DI NOTEBOOK, TABLET E AFFINI 5
4) MANUTENZIONE DEL PERSONAL COMPUTER 5
5) UTILIZZO DELLA POSTA ELETTRONICA 6
6) MODALITA' DI UTILIZZO DELLA RETE INTERNET E DEI RELATIVI SERVIZI 6
7) UTILIZZI PERSONALI CONSENTITI 7
8) MODALITA' DI TRACCIAMENTO DEI DATI 7
9) GESTIONE PASSWORD DI ACCESSO AL PERSONAL COMPUTER, ALLE BANCHE DATI ED ALLA VPN 8
10) MODALITA' DI PROTEZIONE DA MALWARE E VIRUS INFORMATICI 9
11) MODALITA' DI GESTIONE DEI SUPPORTI RIMOVIBILI 9
12) MODALITA' DI UTILIZZO DELLE DOTAZIONI TELEFONICHE 10
13) MODALITA' DI GESTIONE DEGLI ARCHIVI CARTACEI 10
14) ACCESSO FISICO AI LOCALI AZIENDALI 11
15) RISERVATEZZA DEI DATI 11
16) PROCEDURA DISCIPLINARE 11
17) APPLICABILITA' A SOGGETTI DIVERSI DAI DIPENDENTI 12
18) ENTRATA IN VIGORE 12
19) ALLEGATO AL REGOLAMENTO INFORMATICO 12
ALLEGATO A 13
ALLEGATO B 14
ALLEGATO C 15
ALLEGATO D 16
ALLEGATO E 17

PREMESSA

La missione aziendale della Immedia SpA prevede per sua natura la gestione, l'elaborazione e la conservazione di dati; tali operazioni possono essere compiuti sia utilizzando apparati di elaborazione che archivi cartacei. Inoltre la progressiva diffusione delle tecnologie informatiche, ed in particolare il libero accesso alla rete internet dai personal computer aziendali, espone Immedia SpA - e le Società del Gruppo che utilizzano in service i sistemi informativi della controllante - a rischi di carattere patrimoniale ed a responsabilità penali con ricadute negative in termini di sicurezza e di immagine dell'Azienda stessa.
Fermo restando che l'utilizzo delle risorse informatiche e telematiche aziendali deve ispirarsi ai principi di diligenza, correttezza e buona fede (principi questi che sono comunque sottesi al rapporto di lavoro), Immedia SpA ha adottato un Regolamento interno diretto a prevenire, ancorché ad evitare, che comportamenti anche inconsapevoli, possano minacciare e/o compromettere la sicurezza nel trattamento dei dati ovvero che comportamenti scorretti distolgano le risorse aziendali dall'uso cui le stesse sono deputate.
Il presente Regolamento si propone quindi di sintetizzare modalità e finalità di utilizzo del sistema di gestione delle informazioni aziendali, disciplinando le condizioni per il corretto utilizzo degli strumenti informatici, telematici e telefonici nonché sulle corrette modalità di tenuta degli archivi cartacei da parte dei dipendenti di Immedia SpA e degli altri soggetti che vengono espressamente a questo autorizzati.

1) AFFIDAMENTO APPARATI TECNOLOGICI NECESSARI ALLO SVOLGIMENTO DEL LAVORO

a) Il personal computer viene affidato al dipendente come uno strumento di lavoro il cui utilizzo viene regolamentato all'Art. 2 del presente regolamento. Tale affidamento viene formalizzato mediante lettera di presa in carico da parte del dipendente, che a partire da quella data diventa affidatario secondo quanto specificato nel presente regolamento.
b) lo smartphone viene affidato al dipendente come uno strumento di lavoro il cui utilizzo viene regolamentato all'Art. 12 del presente regolamento. Tale affidamento viene formalizzato mediante lettera di presa in carico da parte del dipendente, come da allegato "B" che a partire da quella data diventa affidatario secondo quanto specificato nel presente regolamento.
c) Gli apparati di cui alla lettera a) e b) saranno in carico al dipendente fino alla formale restituzione degli stessi apparati e la firma del verbale di riconsegna all'azienda come da allegato "C" al presente regolamento;

2) MODALITA' DI UTILIZZO DEL PERSONAL COMPUTER

a) Il personal computer affidato al dipendente uno strumento di lavoro il cui utilizzo a fini personali è vietato se non in determinate fasce orarie e/o comunque nei limiti di compatibilità cosi come specificati nel successivo art. 7). Ogni utilizzo non inerente L'attività lavorativa, che superi i limiti di cui al successivo punto 6) può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, compromettere la sicurezza dei dati detenuti a vario titolo da Immedia SpA oltreché integrare fattispecie di illecito penale.
b) I dipendenti cui sono assegnati personal computer sono direttamente responsabili della loro custodia e utilizzo. I dipendenti sono tenuti a comunicare tempestivamente all'Amministratore di sistema eventuali furti, e/o danneggiamenti, anche di lieve entità, di tali strumenti, nonché eventuali anomalie di funzionamento che possano pregiudicare il normale esercizio dell'attività lavorativa.
c) I dipendenti, nell'utilizzo degli strumenti informatici assegnati, devono evitare comportamenti che possono anche solo potenzialmente recare danno alle strumentazioni ed alle banche dati.
d) Ogni dipendente che utilizza un personal computer è pienamente responsabile di tutte le azioni che compie sulla rete aziendale. Le azioni eseguite sui server aziendali (accesso a cartelle di rete

condivise o database) sono gestite dall'Amministratore di Sistema coerentemente con i permessi di accesso concessi all'utente (lettura, scrittura, cancellazione e recupero dei dati limitatamente ad un periodo non superiore ai 7 giorni). Qualora venissero effettuate ed individuate indebite azioni di creazione, cancellazione o modifica dei dati, l'Amministratore di Sistema dovrà inoltrare apposita segnalazione alla Ufficio Risorse Umane e Organizzazione e al Responsabile dell' Amministratore di sistema per ogni provvedimento conseguente.

e) Per evitare l'utilizzo del proprio personal Computer da parte di terzi non autorizzati è necessario inserire la password di accesso al computer stesso secondo le modalità di seguito specificate nell'art.9) del presente regolamento. Tale password dovrà essere richiesta sia all'accensione che alla riattivazione dopo una pausa di utilizzo di un tempo massimo di 5 minuti ovvero dopo che il computer è entrato in modalità salvaschermo.
f) Non è consentito installare autonomamente programmi e/o applicazioni come plugins, codec, programmi freeware/shareware etc., provenienti dall'esterno salvo previa esplicita autorizzazione espressa dell'Amministratore di Sistema, in quanto sussiste il grave pericolo di portare virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore. Per Io stesso motivo non e consentito cambiare le configurazioni hardware e software impostate dall'Amministratore di Sistema e/o salvare files non aventi attinenza con la propria attività lavorativa che per dimensione e/o contenuto siano palesemente in contrasto con la funzione chela dotazione informatica assegnata a chiamata a svolgere, fatto salvo quanto previsto dall'art. 7) dello stesso regolamento.
g) Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dall'Amministratore di Sistema. L'inosservanza di questa disposizione pub comportare, oltreché il rischio di danneggiamenti del sistema per incompatibilità con il software esistente, gravi responsabilità anche penali, a carico di Immedia SpA in caso di violazione della normativa posta a tutela dei diritti d'autore (si vedano il D.Lgs 29.12.19992, n. 518 "attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore" e la L. 18.08.2000, n. 248 "nuove norme di tutela del diritto di autore") che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto da diritto d'autore.
h) Non è consentito al dipendente modificare le caratteristiche impostate sul proprio PC, salvo espressa autorizzazione dell'Amministratore di Sistema.
i) II personal computer deve essere spento al termine dell'orario di lavoro prima di lasciare gli uffici. In caso di assenze prolungate (compresa la sosta pranzo) il pc dovrà essere spento ovvero disconnesso, in maniera tale che al primo accesso il sistema chieda L'inserimento di Iogin e password dell'assegnatario.
j) Non è consentita L'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (ad esempio masterizzatori, modem, etc.) se non previa L'autorizzazione espressa dell'Amministratore di Sistema.
k) E' dovere del dipendente che si assenta dal servizio rendere possibile L'accesso ai files residenti nel PC da parte del responsabile dell'area di appartenenza o da altro dipendente da quest'ultimo individuato, qualora sia ritenuto un elemento utile per l'attività dell'ufficio.
l) Tutte le informazioni contenute per PC sono da considerare documentazione di lavoro di proprietà e stretta disponibilità di Immedia SpA nel rispetto della normativa sui diritti d'autore, sui brevetti, sul segreto professionale che i dipendenti siano tenuti a rispettare.
m) I files memorizzati nel PC o altre unità di memorizzazione collegate dovranno essere esclusivamente di pertinenza delle mansioni o comunque delle attività in generale riconducibili alla prestazione lavorativa del singolo dipendente. E' vietato utilizzare le directory di memoria per salvare files non direttamente riferibili alle mansioni comandate se non nei limiti di cui al successive art.7) del presente regolamento.
n) E' vietato stampare files personali utilizzando le stampanti/fotocopiatrici multifunzione aziendali se non nei limiti di cui al successive art. 7). L'attività che supererà i limiti indicati dall'azienda sarà

considerata uso indebito delle strumentazioni di lavoro e sarà segnalata all'ufficio risorse umane per i procedimenti opportuni.

o) E' vietato fotocopiare documenti personali utilizzando le stampanti/fotocopiatrici multifunzione aziendali, se non nei limiti di cui al successive art. 7) del presente regolamento. Anche tale attività sarà considerata uso indebito delle strumentazioni di lavoro e sarà segnalata all'ufficio risorse umane per i procedimenti opportuni.

p) La distrazione ovvero L'utilizzo improprio del PC assegnato dar luogo alle procedure disciplinari previste dall'art. 7 Statuto dei lavoratori e dal vigente Codice Disciplinare.

q) In caso Immedia SpA ravvisi L'utilizzo improprio del PC, assegnato, ai fini di tutelare il patrimonio aziendale o comunque nell'ambito della correttezza delle relazioni intercorrenti tra datore di lavoro e dipendenti darà preventivo avviso generalizzato o circoscritto a dipendenti afferenti L'Area o il Settore in cui e stato rilevato il comportamento anomalo, con L'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite, contrariamente, in caso di reiterazione, potrà previa comunicazione al trasgressore, prelevare il PC ovvero eseguire tutti i controlli ritenuti necessari presso la postazione interessata, compresa la copia dei dati, programmi, files immagazzinati nella memoria interna del PC. Di queste attività dovrà essere data informazione alla Ufficio Risorse Umane e Organizzazione per ogni procedura e/o procedimento inerente.

r) I dati raccolti con le modalità sopra indicate, saranno conservati a norma di legge dal datore di lavoro per il periodo strettamente necessario alla definizione, eventualmente anche in sede contenziosa, di ogni procedura e/o procedimento inerente. AI termine saranno cancellati e/o restituiti al trasgressore nel rispetto della vigente normativa sulla protezione dei dati.

3) MODALITA' UTILIZZO DI NOTEBOOK, TABLET E AFFINI

a) II dipendente e responsabile del PC Notebook assegnatogli dall'Azienda e deve custodirlo con la massima cura e diligenza sia durante gli spostamenti che nell'utilizzo nel luogo di lavoro.

b) Ai PC Notebook si applicano esattamente le stesse regole relative ai PC di postazione fissa, con particolare riferimento all'utilizzo di programmi/files non autorizzati o comunque non inerenti l'attività lavorativa del dipendente assegnatario ed al loro uso indebito.

c) I PC Notebook utilizzati in occasione di eventi/attività esterne (convegni, visite in azienda, etc.), in caso di allontanamento temporaneo dell'assegnatario, dovranno essere custoditi in luogo protetto.

d) II dipendente assegnatario di un PC Notebook che, venendo meno al dovere di diligenza nella custodia, causi il danneggiamento o smarrimento delle dotazioni informatiche affidate, risponde personalmente del danno patrimoniale arrecato.

e) Trattandosi di apparecchiature che possono per loro natura essere smarrite e/o rubate, deve essere impostata su tali apparati un pin di sblocco dell'avvio del sistema operativo affinché sullo stesso apparato non sia immediatamente leggibile tutto quanto vi sia contenuto. Per le modalità di gestione di tale pin si rimanda all'Art. 9).

4) MANUTENZIONE DEL PERSONAL COMPUTER

Se, nell'ambito dell'attività manutentiva, anche in telediagnosi, verrà riscontrato L'utilizzo di programmi, files, etc. non previsti e/o non afferenti l'attività lavorativa o comunque eccedenti i limiti di compatibilità di cui al successivo art.7), II Responsabile dell'Amministratore di sistema dovrà inoltrare apposita segnalazione all' Ufficio Risorse Umane e Organizzazione per ogni procedura e/o procedimento inerente.

5) UTILIZZO DELLA POSTA ELETTRONICA

a) La casella di posta elettronica assegnata dall'azienda al dipendente è uno strumento di lavoro il cui utilizzo per fini personali non è consentito se non nei limiti di cui al successivo art. 7) del presente regolamento. I dipendenti assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

b) Le caselle di posta elettronica aziendale di tipo "*cognome*@halleyconsulting.it' vanno utilizzate esclusivamente per l'invio di messaggi attinenti il rapporto di lavoro. Ne è vietato l'utilizzo per la partecipazione a dibattiti, forum, chat o mail-list, salvo diversa esplicita autorizzazione dall'Amministratore del Sistema. Per la trasmissione di files attinenti l'attività lavorativa è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e allegati ingombranti.

c) E' obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di files eseguibili o documenti di siti Web o Ftp non conosciuti).

d) E' vietato inviare catene telematiche. Non si devono in alcun caso attivare gli allegati ai messaggi in questione.

e) La casella di posta elettronica, in quanto avente le caratteristiche di cui alla precedente lett. a), non e da intendersi come corrispondenza privata del singolo dipendente ma esclusivamente quale corrispondenza e documentazione di lavoro di stretta pertinenza aziendale. Qualora l'Amministratore di Sistema nell'espletamento delle proprie funzioni individui comportamenti anomali potenzialmente pericolosi per i sistemi informativi aziendali, il datore di lavoro potrà inviare un avviso generalizzato o circoscritto a dipendenti afferenti l'area o il settore in cui stato rilevato il comportamento anomalo con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite, contrariamente il datore di lavoro potrà effettuare controlli sulla singola casella di posta elettronica, anche tramite propri incaricati, con identificazione del mittente, del destinatario e dell'oggetto di ogni mail.

f) E' vietato l'invio di messaggi di posta elettronica interna ad un numero indistinto di utenti (tutti gli utenti o liste di distribuzione), salvo i casi di comprovata necessità organizzativa che andranno appositamente e preventivamente autorizzati.

g) I dipendenti sono responsabili del contenuto delle proprie comunicazioni e della riservatezza dei dati ivi contenuti, la cui impropria colpevole diffusione potrebbe integrare L'illecito di violazione del segreto d'ufficio e/o della normativa in materia di tutela dei dati personali.

6) MODALITA' DI UTILIZZO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

a) II PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento dell'attività lavorativa ed il suo utilizzo per fini personali o comunque non attinenti alle mansioni svolte vietato. E' proibita la navigazione in Internet per motivi diversi da quelli legati alla prestazione lavorativa del dipendente assegnatario del PC abilitato se non nei limiti di cui al successivo art. 7) del presente regolamento.

b) E' fatto divieto all'utente di effettuare il download di software anche se gratuito (freeware) e shareware prelevato da siti internet non certificati dall'Amministratore di Sistema, se non espressamente autorizzato dallo stesso.

c) E' vietata l'effettuazione di ogni genere di transazione finanziaria se non nei limiti di cui al successivo art. 7), ivi comprese le operazioni di remote banking, acquisti on line e simili, salvo i casi direttamente autorizzati dal Responsabile dell'aera di competenza e con il rispetto delle normali procedure di acquisto.

d) Non è consentita ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

e) E' vietata la partecipazione a forum non professionali, social network, gaming on line, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (nickname).
f) E' vietato l'accesso a siti a pagamento, salvo per necessità esclusivamente aziendali.
g) Il dipendente non e in ogni caso autorizzato a produrre ed a pubblicare siti web personali mediante la rete aziendale.
h) L'utilizzo di Internet per scopi attinenti le mansioni di lavoro è ammesso ed autorizzato solo attraverso la rete di trasmissione dati aziendale.
i) L'Amministratore di Sistema provveder a monte, tramite apposite procedure, ad impedire l'accesso ai siti internet di consultazione comune, ai social network (facebook o similari), etc. L'indebito utilizzo del servizio internet da parte del dipendente abilitato comporterà l'avvio di ogni procedura e/o procedimento inerente.

7) UTILIZZI PERSONALI CONSENTITI

Nel convenire che internet e posta elettronica fanno ormai parte della vita quotidiana e che sempre più servizi vengono gestiti con la modalità web, Immedia SpA riconosce la possibilità ai destinatari del presente Regolamento di utilizzare le dotazioni aziendali assegnate, anche per fini personali, purché nel rispetto delle prescrizioni sotto indicate:

a) le connessioni ad internet di carattere non strettamente lavorativo dovranno avvenire fuori orario di lavoro e quindi durante la pausa pranzo ovvero dopo la fine del servizio;
b) per i lavoratori che non hanno l'obbligo di timbratura ci si riferisce, per la determinazione dell'orario di lavoro, a quello standard;
c) sono consentite le connessioni per consultazioni varie, la possibilità di effettuare transazioni bancarie nonché di stampare documenti e/o atti purché in misura ragionevole e non indiscriminata e sempre nei limiti di cui al punto a);
d) l'utilizzo personale della posta elettronica aziendale è consentito sempreché il numero di mail inviate a titolo personale risulti essere di modesta entità rispetto a quelle gestite a livello lavorativo.

Tutte le attività sopra indicate dovranno ispirarsi ai principi di buona fede contrattuale, non dovranno superare la soglia della ragionevolezza né procurare danni e/o costi ulteriori alle dotazioni aziendali.
L'utilizzatore risponderà di eventuali danni arrecati o di un uso ingiustificatamente esteso delle citate attività.

8) MODALITA' DI TRACCIAMENTO DEI DATI

a) Immedia SpA, anche in esecuzione delle prescrizioni di cui al Provvedimento Garante per la Protezione dei Dati Personali del 27.11.2008 ed s.m.i. è dotata di appositi programmi di tracciabilità e conservazione dei dati e delle operazioni che vengono eseguite dagli Amministratori di Sistema, nominati con lettera di incarico a firma del Titolare del Trattamento, come indicate nel D.P.S. vigente, (nel presente regolamento definiti "Amministratore di Sistema") su tutti i server/PC, collegati alla rete aziendale. Le operazioni compiute da tutti gli utenti (dipendenti/collaboratori, etc.), memorizzate dal sistema operativo, vengono conservate per le finalità di cui alle disposizioni normative in materia e al fine di essere rese disponibili a fronte di richieste da parte dell'Autorità Giudiziaria. Unicamente agli Amministratori di Sistema è consentito effettuare operazioni sui dati memorizzati.
b) Considerata l'importanza strategica dei server, che costituiscono la banca dati della Società e quindi il patrimonio imprescindibile per il corretto svolgimento delle attività aziendali che deve essere adeguatamente preservato, l'Amministratore di Sistema è autorizzato ad intervenire

immediatamente al verificarsi di qualsiasi anomalia causata da comportamenti ed usi impropri da parte degli operatori .

c) Le operazioni difformi compiute dall'operatore in seguito individuato, saranno oggetto di segnalazione alla Ufficio Risorse Umane e Organizzazione per i conseguenti procedimenti disciplinari.

d) Le operazioni collegate all'utilizzo della casella di posta elettronica aziendale vengono altresì monitorate tramite apposito log da parte del fornitore del servizio, nel rispetto delle disposizioni di legge in materia. La tracciabilità riguarda solamente i dati identificativi del mittente, destinatario, data e ora di spedizione/ricezione del messaggio e oggetto della missiva.

e) Ogni nuovo accesso a internet deve essere richiesto ed autorizzato da parte del Responsabile competente. L'Amministratore di Sistema provvede all'attivazione del servizio.

f) Ad ogni nuovo dipendente abilitato al servizio internet e/o alla casella di posta elettronica sarà preventivamente consegnata una nota informativa della Direzione contenente "Diritti e Doveri del dipendente" in materia di utilizzo del servizio internet aziendale (Allegato "A" al presente Regolamento), da sottoscriversi per ricevuta. La sottoscrizione vale quale presa d'atto delle informazioni e delle disposizioni normative e di legge a presupposto del presente Regolamento. La mancata sottoscrizione non esonera dalle responsabilità previste per ogni utilizzatore da dette disposizioni normative e/o da norme generali e specifiche adottate dall'Azienda.

g) Ogni nuovo accesso alla rete aziendale a favore di personale NON dipendente (collaboratori, consulenti, stagisti, etc.) dovrà essere espressamente richiesto dal Responsabile competente.

9) GESTIONE PASSWORD DI ACCESSO AL PERSONAL COMPUTER, ALLE BANCHE DATI ED ALLA VPN

a) Tutti i dipendenti/collaboratori che per lo svolgimento del proprio lavoro (previa richiesta tramite gli allegati "A" ed "E" del presente Regolamento), sono messi a conoscenza di password per l'accesso alle banche dati aziendali, reti Lan e/o wi-fi, accesso alle procedure di back-office interne all'azienda e/o Server dei Clienti, sono tenuti ai sensi della normativa vigente a mantenere la segretezza di tali password, ogni accertata violazione a questo esplicito punto verrà segnalato alla Direzione del Personale per dar luogo alle procedure disciplinari previste dall'art. 7 dello Statuto dei lavoratori e dal vigente Codice Disciplinare

b) Il vincolo alla segretezza sopracitato nel punto a) ai sensi della normativa vigente permane anche al cessare del rapporto di lavoro, pertanto ogni accertata violazione in tal senso verrà perseguita presso le opportune sedi.

c) Tutti i dipendenti devono impostare una password di accesso al sistema operativo della propria postazione sia essa un PC fisso che un notebook. Tale password deve essere composta da almeno 8 caratteri alfanumerici e contenere almeno una lettera Maiuscola ed un segno di punteggiatura così come raccomandato dal D.Lgs 196/2003.

d) i dipendenti dotati di Notebook sono tenuti ad impostare un pin all'accensione del sistema per evitare che terzi possano accedere ai dati in esso contenuti quando tale apparato si trovi fuori dall'azienda.

e) Le password di accesso alle procedure di back-office avranno scadenza semestrale e saranno rilasciate la prima volta a cura dell'Amministratore del Sistema mediante comunicazione formale a ciascun operatore che ne faccia richiesta tramite il proprio responsabile, dopo di che avranno scadenza automatica.

f) Le password di accesso alle reti VPN avranno scadenza semestrale e saranno rilasciate a cura dell'Amministratore del Sistema mediante comunicazione formale a ciascun operatore che ne faccia richiesta tramite il proprio responsabile.
g) Le password di accesso alle reti Wi-Fi avranno scadenza semestrale e saranno rilasciate a cura dell'Amministratore del Sistema mediante comunicazione formale a ciascun operatore che ne faccia richiesta tramite il proprio responsabile.
h) Le password di Amministrazione dei Server e degli apparati di rete saranno custodite dall'amministratore di rete e potranno essere comunicate a chi si occuperà della manutenzione dei sistemi in sua sostituzione.

10) MODALITA' DI PROTEZIONE DA MALWARE E VIRUS INFORMATICI

a) Ogni dipendente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus od altro software aggressivo.
b) E' buona norma per il dipendente controllare il regolare funzionamento e l'aggiornamento periodico del software antivirus installato secondo le procedure previste.
c) Nel caso il software antivirus rilevi la presenza di virus, l'utente dovrà immediatamente:
   1) sospendere ogni elaborazione in corso senza spegnere il computer;
   2) segnalare l'accaduto all'amministratore di sistema;
d) Ogni dispositivo magnetico di provenienza esterna all'azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso un virus venga rilevato, dovrà essere consegnato all'amministratore di sistema.
e) Non è consentito l'utilizzo di floppy disk, cd rom anche riscrivibili, dvd, nastri magnetici, USB key, hard disk esterni, unità di memoria di massa esterne o altro dispositivo di memorizzazione di provenienza ignota.

11) MODALITA' DI GESTIONE DEI SUPPORTI RIMOVIBILI

a) I supporti rimuovibili quali: floppy disk, cd rom riscrivibili, dvd riscrivibili, nastri magnetici, USB key, hard disk esterni, unità di memoria di massa esterne o altro dispositivo di memorizzazione che vengono utilizzati per trasportare dati sensibili,personali o giudiziari interni all'azienda e/o dei Clienti per qualsiasi elaborazione, dovranno essere gestiti secondo il seguente metodo:
   i) Redigere un apposito registro di ingresso in azienda di tali dati su supporto opportunamente identificato, la tenuta di tale registro sarà effettuata a carico dell'amministratore di sistema
   ii) Conservare detto supporto in un luogo fisicamente protetto da eventuali furti e/o manomissione dei dati, tale luogo di conservazione sarà indicato nel registro di cui al punto a).
   iii) Una volta terminata l'elaborazione che ha richiesto il trasporto di tali dati, il contenuto del supporto rimuovibile dovrà essere eliminato mediante strumenti che azzerino fisicamente il contenuto del supporto stesso, quali strumenti di formattazione a basso livello dei supporti; Per i supporti che non possano essere formattati a basso livello quali CD-ROM o DVD, dovranno essere fisicamente distrutti; l'avvenuta formattazione/distruzione del supporto sarà indicata nel registro di cui sopra la cui tenuta sarà effettuata a carico dell'amministratore di sistema.

12) MODALITA' DI UTILIZZO DELLE DOTAZIONI TELEFONICHE

a) lo Smartphone aziendale oltreché la postazione fissa rappresentano dotazioni elettroniche/telematiche finalizzate o comunque concorrenti a migliorare e/o a facilitare Io svolgimento delle mansioni affidate al dipendente.
b) II personale dipendente assegnatario ne deve avere cura, segnalando ogni anomalia di funzionamento all'amministratore di sistema.
c) AI dipendente assegnatario di telefono fisso e/o mobile fatto espresso divieto di:
   i) manomettere i componenti dell'apparecchio;
   ii) effettuare operazioni di programmazione non previste dal manuale d'uso;
   iii) collegare apparecchiature non espressamente autorizzate dall'amministratore di sistema (ad es. segreteria telefoniche o altro);
   iv) effettuare chiamate per dettatura di telegrammi (salvo utenti espressamente autorizzati);
   v) alterare l'apparecchio con pennarelli indelebili o altro (si invalida la garanzia).
d) AI dipendente assegnatario di smartphone è fatto espresso divieto di:
   i) rimuovere la SIM dal telefono mobile aziendale per installarla su apparecchio diverse rispetto a quello assegnato, salvo casi di temporanea necessità;
   ii) utilizzare il telefono in dotazione per uso personale o comunque per fini diversi da quelli aziendali salvo quanto specificato nell'Art. 7 del presente regolamento;
   iii) utilizzare la connessione internet ovvero la gestione di messaggi di posta elettronica per gli apparecchi dotati delle citate funzionalità per scopi differenti a quelli lavorativi.
e) L'uso indebito delle dotazioni telefoniche aziendali comporterà, a carico del trasgressore, l'apertura a suo carico di una procedura disciplinare.
f) II dipendente assegnatario che, venendo meno al dovere di diligenza di cui alla precedente lettera b), causi la perdita (smarrimento) e/o il danneggiamento delle dotazioni telefoniche affidate, risponderà patrimonialmente del danno arrecato se, nell'arco di due anni, avrà perso o reso inservibile due apparati. All'assegnazione del terzo apparecchio (fisso e/o mobile) il relativo costo sarà addebitato a cedolino paga.

L'azienda utilizza sia a propria tutela che per un efficace controllo dei costi un sistema di documentazione addebiti telefonici che archivia tutte le telefonate uscenti ed i costi generati dal singolo telefono aziendale. L'archivio rispetta le normative di tutela della privacy omettendo l'indicazione delle ultime tre cifre del numero chiamato.

13) MODALITA' DI GESTIONE DEGLI ARCHIVI CARTACEI

La gestione, l'elaborazione e la conservazione dei dati, sia pertinenti l'azienda stessa che dati provenienti dai Clienti, possono essere compiute anche utilizzando degli archivi cartacei, scopo del presente punto è regolamentare la modalità di tenuta di questi archivi. Gli archivi cartacei possono essere suddivisi in due macrocategorie ovvero dati cui tutti i dipendenti possono avere accesso nello svolgimento del proprio lavoro e dati il cui accesso è consentito soltanto ad alcune figure specifiche ben identificate e non all'interezza dei dipendenti aziendali.

a) Gli archivi cartacei cui tutti i dipendenti possono avere accesso riguardano la gestione delle commesse di lavoro, la pianificazione ed utilizzo di strumenti aziendali, la gestione delle comunicazioni non riservate intercorse con i Clienti, nonché ogni qualsiasi altra informazione non contenente dati sensibili, personali e/o giudiziari. Tali informazioni possono essere contenute all'interno di contenitori (armadi, cassettiere, ecc.) che non siano fisicamente chiuse e che possono essere accedute da chiunque abbia accesso ai locali. Tali dati possono essere rilasciati a chiunque ne abbia necessità nell'ambito dello svolgimento delle proprie mansioni di lavoro.

b) Gli archivi cartacei il cui accesso è consentito soltanto ad alcune figure specifiche ben identificate e non all'interezza dei dipendenti aziendali riguardano Dati del Personale, Dati afferenti la Contabilità, Contratti dei fornitori, Contratti con i Clienti, Fatture originali, Dati Sensibili dei Clienti nonché ogni qualsiasi altra informazione contenente dati sensibili, personali e/o giudiziari. Tali informazioni possono essere contenute solamente all'interno di contenitori (armadi, cassettiere, ecc.) che siano fisicamente chiuse e che non possono essere accedute da chiunque abbia accesso ai locali. L'accesso a tali dati può essere effettuato soltanto alle persone ben specifiche identificate come gestori di tali informazioni e alle stesse verranno rilasciate le chiavi di apertura dei contenitori degli archivi.

14) ACCESSO FISICO AI LOCALI AZIENDALI

Gli accessi fisici ai locali aziendali sono consentiti soltanto al personale dipendente ed ad altri soggetti come meglio specificati al punto 17 del presente Regolamento.
E' consentito inoltre l'accesso ai Fornitori, Clienti, visitatori che per esigenze aziendali debbano svolgere attività all'interno dell'azienda; per questi soggetti è stato istituito un Registro degli Accessi presso la segreteria di sede nonché la consegna di un badge di riconoscimento.
Per l'accesso ai locali che per loro natura contengono informazioni riservate, sono previste apposite autorizzazioni e/o nomine di personale autorizzato all'accesso.

15) RISERVATEZZA DEI DATI

a) Per "informazioni Riservate" si intendono tutte le informazioni di qualsivoglia natura riferite od apprese in occasione dello svolgimento delle mansioni per le quali il dipendente stato assunto da Immedia SpA spa. II dipendente stesso si impegna a non comunicarle e/o divulgarle se non per ragioni connesse all'attività lavorativa e nel rispetto della vigente normativa sulla protezione dei dati personali e ad adottare tutte le misure ragionevolmente necessarie per non pregiudicarne la riservatezza.
b) II dipendente si impegna ad utilizzare le Informazioni Riservate unicamente allo scopo di effettuare l'attività lavorativa cui e preposto e di conseguenza a non usare tali informazioni per altre finalità e/o in maniera tale che dalla diffusione delle stesse possa derivare un qualsiasi danno alla società.
c) II presente regolamento si applica, in quanto compatibile, ai dipendenti Immedia SpA iscritti ad Albi Professionali che svolgano per Immedia SpA medesima attività inerenti la relativa iscrizione, nel rispetto delle disposizioni normative, anche deontologiche, applicabili ai rispettivi ordini professionali o comunque alla specifica attività professionale svolta.
d) Immedia SpA risolverà eventuali contrasti circa I'utilizzo e la conservazione dei dati, anche sensibili, derivanti dalla natura delle attività professionali svolte, applicando le citate disposizioni normative.

16) PROCEDURA DISCIPLINARE

a) II presente Regolamento è vincolante per tutti i soggetti che comunque utilizzino reti e/o risorse informatiche e/o telematiche di Immedia SpA
b) Di esso sarà data adeguata conoscenza anche attraverso la pubblicazione sul portale di Immedia SpA
c) In esso sono richiamati i doveri del personale dipendente in ordine al rispetto della politica del sistema di sicurezza per le informazioni. Le responsabilità ed i doveri relativi alla gestione della sicurezza delle informazioni rimangono validi anche dopo la cessazione del rapporto di lavoro.

d) Il mancato rispetto delle regole contenute nel presente Regolamento comporterà l'instaurazione di ogni procedimento e/o procedura inerente impregiudicata ogni responsabilità civile e penale discendenti dal medesimo fatto.

17) APPLICABILITA' A SOGGETTI DIVERSI DAI DIPENDENTI

a) Tutte le disposizioni del presente Regolamento si applicano, in quanto compatibili, anche a soggetti diversi dai lavoratori dipendenti (collaboratori, consulenti, stagisti, etc.) che a vario titolo utilizzano la rete di Immedia SpA e/o risultano essere assegnatari di dotazioni informatiche/telematiche, telefoniche nonché di accesso agli archivi cartacei aziendali.

18) ENTRATA IN VIGORE

a) Il presente Regolamento è soggetto a modifiche ed aggiornamenti
b) Il Presente Regolamento ed ogni suo aggiornamento avranno efficacia trascorso un mese dalla data di pubblicazione dello stesso o dell'aggiornamento sul portale aziendale.
c) Nelle more dell'entrata in vigore del presente Regolamento e di ogni suo aggiornamento, ogni dipendente assegnatario di PC, PC portatile etc. dovrà verificare la congruità dei programmi, files, salvati all'interne delle apparecchiature affidate e provvedere alla cancellazione del materiale considerato difforme da quanto previsto dal Regolamento medesimo.

19) ALLEGATO AL REGOLAMENTO INFORMATICO

a) Costituisce parte integrante del presente Regolamento la nota di cui all'Allegato A).
b) La nota di cui all'allegato A) dell'art. 7, punto h) del Regolamento vigente antecedentemente al sopraesteso aggiornamento da intendersi quale mera informativa circa i diritti e doveri che fanno capo al dipendente/collaboratore e/o dipendente di società controllate che utilizza strumenti informatici collegati con i server aziendali. L'avvenuta sottoscrizione "per accettazione" e da ritenersi valida ai soli fini della attestazione di ricevimento della nota stessa.

ALLEGATO A

Luogo e data _____

All'Amministratore di Sistema

OGGETTO: Richiesta di accesso al servizio intranet/Internet aziendale e/o alle Banche Dati

Il sottoscritto _____ in qualità di Responsabile dell'Area _____

CHIEDE

per il dipendente/collaboratore _____ l'accesso ai seguenti servizi/banche dati:

- ☐ Accesso alla rete Internet/Intranet;
- ☐ Accesso alla rete wi-fi;
- ☐ Accesso VPN;
- ☐ Accesso al server telefonico Voip;
- ☐ Accesso al gestione di back-office aziendale;
- ☐ Accesso al gestionale per l'assistenza;
- ☐ Accesso al gestionale della Contabilità;
- ☐ Accesso al gestionale delle Risorse Umane;
- ☐ Altro (specificare)

Diritti e Doveri del dipendente/collaboratore

1. Il dipendente/collaboratore prende atto dell'esistenza del registro dei collegamenti (log) mantenuto da sistema anti
intrusione.
2. Il dipendente/collaboratore prende atto che Halley Consulting S.p.A., adotta tutte le misure tecniche ed organizzative necessarie a garantire la riservatezza del registro degli eventi.
3. Il dipendente/collaboratore prende atto che il registro degli eventi potrà essere esibito su richiesta dell' Autorità Giudiziaria .
4. Il dipendente/collaboratore tenuto, nell'utilizzo del servizio, al rispetto delle vigenti disposizioni normative e di legge
in materia.
5. Il dipendente/collaboratore dà atto di essere informato sul contenuto del Regolamento Aziendale vigente per l'utilizzo del Sistema Informativo e sulle vigenti disposizioni normative e di legge che ne disciplinano l'uso.

Il responsabile	Il dipendente/collaboratore	L'Amministratore di sistema
_____	_____	_____
(firma per ricevuta)	(firma per ricevuta)	(firma per ricevuta)

ALLEGATO B

VERBALE DI CONCESSIONE IN USO E CONSEGNA TELEFONO CELLULARE E/O LAPTOP

La società IMMEDIA SPA SPA nella veste del suo rappresentante legale _____,

CONCEDE in USO e CONSEGNA

al Sig. ……., dipendente/collaboratore (barrare quanto non pertinente) della società;

il cellulare/laptop/tablet/altro ((barrare quanto non pertinente)) tipo ……..

serial number ……..

alle seguenti condizioni:

- ☐ l'uso si intende autorizzato dal ../../…. fino ad eventuale reso che avverrà previa compilazione del mod. M205-Verbale di restituzione apparati;
- ☐ i beni sopra descritti debbono servire per adempiere le mansioni lavorative assegnate al dipendente;
- ☐ sono a carico della società gli oneri di riparazione e le spese derivanti dall'utilizzo dei suddetti beni;
- ☐ il dipendente si obbliga a custodire ed utilizzare i beni in oggetto secondo le indicazioni del "Regolamento Utilizzo Sistema Informativo interno" (consultabile sul portale aziendale o presso l'ufficio Risorse Umane) che con la presente lettera firmata per accettazione si intende accolto in ogni sua parte.

Catania, il ../../….

La società Il dipendente per accettazione

…… ……..

ALLEGATO C

VERBALE DI RESTITUZIONE APPARATI

La società IMMEDIA SPA nella veste del suo rappresentante legale GRAZIA PARISI,

RIPRENDE IN CARICO

il cellulare/laptop/tablet/altro (specificare) …….

tipo …….. serial number ……

attualmente in carico al Sig. ……..,

dipendente/collaboratore (barrare la scelta errata) della società per il seguente motivo (selezionare il caso corretto):

- ☐ sostituzione per obsolescenza o guasto non riparabile;
- ☐ restituzione volontaria;
- ☐ cambio di mansione;
- ☐ fine del rapporto di lavoro;
- ☐ altro (specificare) ……..

Catania, il ../../….

La società Il dipendente/collaboratore per accettazione

M205 Rev.01 del 02/11/2017

ALLEGATO D

NOMINA AMMINISTRATORE DI SISTEMA

Egregio signor/a ….

La società Immedia SPA, nella persona del legale rappresentante _____, dopo aver valutato la Sua competenza in materia di misure di sicurezza informatiche

la nomina

Amministratore di Sistema.

Nella qualità di Amministratore di Sistema ha il compito di:

- adottare le misure di sicurezza informatiche indicate dalla legge e vigilare sul loro buon funzionamento e sulla corretta applicazione
- attribuire ad ogni incaricato le credenziali di autenticazione (*username* e *password*), e verificarne il corretto uso e sostituzione;
- verificare l'efficacia delle protezioni antivirus installate e degli altri sistemi di protezione eventualmente necessari;
- predisporre con la dovuta frequenza le copie di back-up o delegare a ciò un incaricato
- predisporre un sistema di registrazione dei Suoi accessi logici ai sistemi informatici, che consentano di risalire al tempo e alle modalità di accesso.

La preghiamo di restituirci copia della presente, firmata per accettazione.

Cordiali saluti.

……, lì, …….

L'Amministratore Unico

_____

Il dipendente per ricevuta

_____

ALLEGATO E

VERBALE DI CONCESSIONE ACCESSO VPN

La società IMMEDIA SPA nella veste del suo rappresentante legale GRAZIA PARISI ,

CONCEDE in USO e CONSEGNA

al Sig. ……, dipendente o collaboratore della società il certificato digitale per la connessione in VPN (Virtual Private Network) alla rete aziendale da esterno.

Da Computer □ Da smartphone □

Tale concessione avviene alle seguenti condizioni:

- ☐ l'uso si intende autorizzato dal ...../...../…….. fino ad eventuale cessazione;
- ☐ l'uso può essere revocato in qualsiasi momento e ad insindacabile giudizio dalla direzione per motivi di sicurezza dei dati;
- ☐ l'accesso sopra descritto deve essere utilizzato esclusivamente per adempiere le mansioni lavorative assegnate al dipendente/collaboratore;
- ☐ l'utilizzo dell'accesso VPN potrà essere tracciato per motivi di sicurezza dei dati;
- ☐ il dipendente/collaboratore si obbliga a custodire ed utilizzare quanto in oggetto secondo le indicazioni del "Regolamento Utilizzo Sistema Informativo interno" (consultabile sul portale aziendale o presso l'ufficio Risorse Umane) che con la presente lettera firmata per accettazione si intende accolto in ogni sua parte.

- Il dipendente/collaboratore richiede di ricevere il certificato VPN sulla propria casella email (indicare quale) .....

- Il dipendente/collaboratore richiede di aver installato il certificato VPN da un tecnico dell'area sistemi sul proprio elaboratore/smartphone: SI □ NO□

Catania li ...../...../.....

La direzione	Il Responsabile	Il Dipendente/collaboratore