

**REGOLAMENTO AZIENDALE IN MATERIA DI PRIVACY**

**Sommario**

<b>1. SCOPO .....</b>	<b>3</b>
<b>2. CAMPO DI APPLICAZIONE .....</b>	<b>3</b>
<b>3. RIFERIMENTI.....</b>	<b>3</b>
<b>4. FINALITÀ.....</b>	<b>4</b>
<b>5. OBBLIGHI DI ARS SERVICE S.R.L. ....</b>	<b>5</b>
<b>6. OBBLIGHI PER I LAVORATORI E COLLABORATORI .....</b>	<b>6</b>
<b>7. USO PROFESSIONALE.....</b>	<b>6</b>
<b>8. PROTEZIONE CONTRO FURTI E DANNEGGIAMENTI.....</b>	<b>6</b>
<b>9. RISERVATEZZA E PROTEZIONE DEL SISTEMA E DEI DATI .....</b>	<b>7</b>
<b>10. POLITICHE DI CLEAR DESK E CLEAR SCREEN.....</b>	<b>7</b>
<b>11. INTEGRITÀ E DISPONIBILITÀ DEI DATI (CARTELLE DI RETE).....</b>	<b>8</b>
<b>12. UTILIZZO DEL PERSONAL COMPUTER .....</b>	<b>8</b>
<b>13. MODALITÀ DI ACCESSO ALLE POSTAZIONI DI LAVORO .....</b>	<b>9</b>
<b>14. CONTINUITÀ DELL'ATTIVITÀ LAVORATIVA IN CASO DI ASSENZA DEL LAVORATORE/COLLABORATORE/UTENTE .....</b>	<b>10</b>
<b>15. UTILIZZO DELL'ELABORATORE E DELLA RETE INTERNA.....</b>	<b>10</b>
<b>16. MODALITÀ DI GESTIONE DELLE PASSWORD .....</b>	<b>12</b>
<b>a) Istruzioni per scegliere la password.....</b>	<b>12</b>
<b>b) Regole di conservazione della password .....</b>	<b>12</b>
<b>17. NAVIGAZIONE IN INTERNET .....</b>	<b>13</b>
<b>18. USO DELLA POSTA ELETTRONICA AZIENDALE .....</b>	<b>15</b>
<b>19. CONTINUITÀ NELL'USO DELLA CASELLA DI POSTA ELETTRONICA IN CASO DI ASSENZA DEL LAVORATORE .....</b>	<b>16</b>
<b>20. CONTINUITÀ NELL'USO DELLA CASELLA DI POSTA ELETTRONICA IN CASO DI FERIE DEL LAVORATORE DELEGATO .....</b>	<b>16</b>
<b>21. PROTEZIONE ANTIVIRUS.....</b>	<b>17</b>
<b>22. UTILIZZO DI APPARATI PER LA TELEFONIA MOBILE .....</b>	<b>17</b>
<b>23. UTILIZZO DI PC PORTATILI.....</b>	<b>18</b>
<b>24. UTILIZZO DI SUPPORTI MAGNETICI.....</b>	<b>18</b>

25. TELEASSISTENZA ..... 19

26. MEMORIZZAZIONE FILE DI LOG DELLA NAVIGAZIONE INTERNET ..... 19

27. TRASMISSIONE E RIPRODUZIONE DEI DOCUMENTI ..... 19

28. MISURE DI SICUREZZA PER IL TRATTAMENTO DI DATI PERSONALI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI..... 20

29. MISURE DI SICUREZZA PER IL TRATTAMENTO DI DATI SENSIBILI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI..... 21

30. MISURE DI SICUREZZA PER IL TRATTAMENTO DI DATI SENSIBILI CON L'AUSILIO DI STRUMENTI ELETTRONICI..... 21

31. DISTRUZIONE DOCUMENTI CARTACEI ..... 22

32. CONTROLLI E MONITORAGGIO DELLE RISORSE ..... 22

33. NON OSSERVANZA DELLA NORMATIVA AZIENDALE ..... 24

34. DENUNCIA AUTORITÀ GIUDIZIARIA..... 24

00	01/08/19	Prima emissione	Responsabile Trattamento dati	Titolare del Trattamento
<i>rev.</i>	<i>Data</i>	<i>motivo revisione</i>	<i>redazione e verifica</i>	<i>approvazione</i>
01				

## **1. SCOPO**

Il presente Regolamento aziendale ha lo scopo di definire le regole di comportamento da adottarsi nell'utilizzo di tutte le dotazioni informatiche e telematiche, nonché delle regole di comportamento da adottarsi nell'utilizzo della documentazione nell'ambito di **ARS SERVICE S.R.L** ai fini di conformarsi in materia di privacy a quanto prescritto dal Regolamento UE 2016/679 e dalla legislazione tutta vigente in tale materia.

## **2. CAMPO DI APPLICAZIONE**

Il presente Regolamento si applica:

- a tutti i Dipendenti, Collaboratori, Consulenti e a chiunque abbia in dotazione, anche temporaneamente, risorse informatiche e telematiche di proprietà di ARS SERVICE S.R.L o ad essa affidate;
- a coloro che svolgano, a qualsiasi titolo, attività per conto di ARS SERVICE S.R.L, accedendo al sistema informatico o utilizzando dotazioni informatiche e/o telematiche di quest'ultima;
- a tutte le attività o comportamenti comunque connessi all'utilizzo della rete Internet e della posta elettronica, mediante strumentazione aziendale della ARS SERVICE S.R.L o di terze parti autorizzate all'uso dell'infrastruttura aziendale.

Le disposizioni contenute nel presente Regolamento sono dirette a garantire la sicurezza, la disponibilità e l'integrità dei sistemi informatici nel rispetto dei principi e delle misure di sicurezza di cui al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, nonché alla normativa vigente tutta.

## **3. RIFERIMENTI**

- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
- Legge n.547 del 23/12/93 "Modificazioni ed integrazioni delle norme del codice penale e del codice di procedura penale in tema di criminalità informatica" e s.m.i. – Altra normativa in vigore in materia di criminalità informatica
- Legge. n. 248 del 18/8/2000 - "Nuove norme di tutela del diritto d'autore" e s.m.i. – Altra normativa in vigore in materia di diritto d'autore
- Linee guida Garante Privacy
- Provvedimenti Garante Privacy
- CCNL applicabile (CCNL Autotrasporto merci e logistica).

#### 4. FINALITÀ

Il presente Regolamento viene adottato al fine di garantire la protezione e la salvaguardia del business aziendale di **ARS SERVICE S.R.L.**, in relazione ai fattori e ai comportamenti potenzialmente dannosi per la sicurezza delle informazioni e del Sistema Informativo Aziendale nella sua complessità.

Il presente Regolamento dovrà essere letto e sottoscritto dai Destinatari indicati.

L'utilizzo degli strumenti informatici aziendali da parte degli utenti non potrà avvenire senza aver preventivamente ricevuto e recepito le prescrizioni e le indicazioni ivi contenute.

Il presente Regolamento è applicabile a tutto il Personale previsto al paragrafo 2. e a quanti altri si trovassero a dover utilizzare le dotazioni ICT messe a disposizione da **ARS SERVICE S.R.L.** o comunque tratti documentazione inerente la attività di **ARS SERVICE S.R.L.** alla quale si applichi quanto prescritto dal Regolamento UE 2016/679 e/o dalla legislazione tutta vigente in tale materia. Per dotazione ICT si intende qualsiasi risorsa informatica e/o telematica (es.: computer, software, rete, utenza, file, cartella di rete, internet key, telefono cellulare, modem, ...) che **ARS SERVICE S.R.L.** metta a disposizione ai destinatari del presente Regolamento.

La sicurezza delle informazioni costituisce un valore imprescindibile per l'Azienda e per i suoi Lavoratori, in particolare nell'ambito della postazione di lavoro e dei sistemi informatici aziendali.

Lo scopo del presente Regolamento è quello di indicare i limiti entro cui i fruitori aziendali possono legittimamente usare le postazioni di lavoro ed i servizi Internet, evitando di esporre sé stessi e/o la propria Azienda a gravi conseguenze che, in taluni casi, determinano ingenti sanzioni pecuniarie e, nei casi più gravi, possono investire il diritto penale.

Questo documento è stato implementato in particolare per tutelare la sicurezza dei Sistemi Informativi di **ARS SERVICE S.R.L.** e comunque di tutta la documentazione inerente la attività di **ARS SERVICE S.R.L.** alla quale si applichi quanto prescritto dal Regolamento UE 2016/679 e/o dalla legislazione tutta vigente in tale materia.

I Sistemi Informativi (hardware e software) e i dati aziendali in essi contenuti sono elementi essenziali per il raggiungimento degli obiettivi aziendali di **ARS SERVICE S.R.L.**

Essi sono, inoltre, parte del patrimonio della **ARS SERVICE S.R.L.**

In tal senso, tutte le risorse del sistema, inclusi l'attrezzatura, i programmi e tutti i dati inviati, ricevuti, salvati, e i mezzi di comunicazione resi disponibili sono e rimangono proprietà di **ARS SERVICE.**

Ogni Utente all'interno di **ARS SERVICE S.R.L.** è responsabile nel proprio ambito della protezione delle informazioni e degli strumenti che in qualsiasi modo impiega durante lo svolgimento del proprio lavoro.

Ogni Utente di **ARS SERVICE S.R.L.** deve essere consapevole dell'importanza della sicurezza delle informazioni e deve operare in modo da garantire tale sicurezza.

In nessun caso l'Utente dovrà utilizzare il Sistema Informativo aziendale per commettere un reato.

Per **ARS SERVICE S.R.L.** garantire la sicurezza dei sistemi informativi significa:

- Assicurare la disponibilità delle risorse informative e dei dati.
- Assicurare l'integrità dei sistemi e dei dati.
- Assicurare la riservatezza delle informazioni.

La regolamentazione della materia, ai sensi dell'art.4, comma 1, della L.300/70, non è finalizzata a un controllo a distanza dei lavoratori da parte di **ARS SERVICE S.R.L.**, ma solo a permettere a quest'ultima di utilizzare sistemi informativi per far fronte a esigenze produttive e organizzative, nonché per esigenze di sicurezza nel trattamento dei dati personali.

È garantito al singolo Lavoratore il diritto di accesso ai dati personali che lo riguardano con le modalità previste dalle disposizioni normative e regolamentari vigenti in materia.

## **5. OBBLIGHI DI ARS SERVICE S.R.L.**

I trattamenti effettuati da **ARS SERVICE S.R.L.** rispettano le garanzie poste in essere dal Legislatore in materia di protezione dei dati e si svolgono nell'osservanza dei seguenti principi:

- il principio di necessità, secondo cui, in relazione alle finalità perseguite, i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi;
- il principio di correttezza, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai Lavoratori, in modo da scongiurare l'eventuale svolgimento di trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa ed effettuati all'insaputa o senza la piena consapevolezza dei Lavoratori;
- il principio del trattamento per finalità determinate, esplicite e legittime, osservando il principio di pertinenza e non eccedenza.

In quest'ottica, **ARS SERVICE S.R.L.** tratta i dati dei Lavoratori nella misura meno invasiva possibile, affidando eventuali attività di monitoraggio esclusivamente a quei soggetti opportunamente preposti ed effettuando eventuali controlli esclusivamente in maniera mirata sull'area di rischio, tenuta in debito conto la normativa sulla protezione dei dati e, se pertinente, il principio di segretezza della corrispondenza.

In base al richiamato principio di correttezza, l'eventuale trattamento deve essere ispirato a un principio di trasparenza.

Grava quindi sul Datore di lavoro l'onere di indicare in ogni caso, chiaramente e in modo particolareggiato, quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette, nonché l'onere di indicare se, in che misura e con quali modalità vengano effettuati controlli.

Il presente Regolamento ha l'intento di adempiere a quest'obbligo.

**ARS SERVICE S.R.L.** ha inoltre predisposto tutte le accortezze necessarie affinché i dati personali contenuti nelle postazioni di lavoro informatiche siano protetti contro il rischio d'intrusione – tanto

dall'esterno (Internet) che dall'interno (rete locale) – e dall'azione di programmi di cui all'art. 615-quinquies del codice penale, attraverso l'utilizzazione di idonei strumenti elettronici, mantenuti costantemente aggiornati.

Anche i programmi della postazione di lavoro sono mantenuti costantemente aggiornati, come per legge, al fine di prevenire le vulnerabilità degli strumenti elettronici e a correggerne i difetti (i c.d. bug).

Sono state predisposte, altresì, le opportune istruzioni organizzative e tecniche volte a prevedere il salvataggio dei dati e sono state previste e adottate le opportune procedure volte a garantire il ripristino dell'accesso alle informazioni o agli strumenti elettronici danneggiati in un arco di tempo non superiore ai 7 (sette) giorni.

## **6. OBBLIGHI PER I LAVORATORI E COLLABORATORI**

Di seguito vengono specificati gli obblighi e le norme di condotta obbligatorie per ciascun Lavoratore, Collaboratore e per tutti coloro che, in virtù di un rapporto di lavoro o fornitura, trattano informazioni ovvero utilizzano sistemi informativi o apparecchiature elettroniche di proprietà di **ARS SERVICE**.

## **7. USO PROFESSIONALE**

L'Utente accetta di usare i Sistemi Informativi per scopi professionali in relazione alla propria posizione all'interno di **ARS SERVICE S.R.L.**

Le risorse relative ai Sistemi Informativi non verranno utilizzate per sviluppare o sfruttare programmi/dati a scopo personale o per terzi.

In particolare è proibito:

- Installare/utilizzare software non autorizzati dal Responsabile IT.
- Utilizzare i sistemi aziendali per servizi o comunicazioni illecite o illegali.
- Utilizzare le risorse aziendali per profitto personale.

I lavoratori dovranno quindi custodire diligentemente gli strumenti informatici e telematici ed i programmi, utilizzandoli solamente per fini professionali.

## **8. PROTEZIONE CONTRO FURTI E DANNEGGIAMENTI**

Per assicurare le apparecchiature informatiche dall'accesso non autorizzato, le stesse dovrebbero essere protette portando a termine le sessioni attive e accertandosi che la password di protezione sia attivata quando l'apparecchiatura viene lasciata incustodita (tranne, naturalmente, quando il computer debba rimanere aperto per un motivo specifico).

Ogni apparecchiatura portatile (computer portatili, cellulare, etc.) deve essere custodita in luoghi chiusi a chiave o comunque in luoghi sicuri contro il furto.

Quando essa è utilizzata fuori dell'edificio aziendale, devono essere prese tutte le precauzioni contro il furto, non soltanto delle attrezzature ma anche di tutti i dati riservati e/o importanti salvati sull'apparecchiatura.

L'Utente deve informare subito di qualsiasi danno, furto o perdita di apparecchiatura, software e/o informazioni che gli sono state affidate.

## **9. RISERVATEZZA E PROTEZIONE DEL SISTEMA E DEI DATI**

Nessun Utente può leggere o alterare le e-mail o le informazioni salvate su computer altrui, a meno che l'Utente non sia stato precedentemente autorizzato per iscritto.

L'Utente non è autorizzato ad accedere, né a tentare l'accesso, alle informazioni alle quali non ha normalmente privilegi di accesso. Se per errore, o a causa di un errato funzionamento del sistema, l'Utente ottenesse l'accesso a funzioni o informazioni normalmente non consentitegli, dovrà immediatamente chiudere il programma o il file nel quale è entrato e informare l'Amministratore di sistema riguardo la situazione.

È proibita ogni attività realizzata per violare o per sollecitare la sicurezza del sistema, salvo autorizzazione esplicita da parte dell'Amministratore di sistema.

Gli Amministratori, utenti privilegiati che devono assicurare il corretto funzionamento e la sicurezza della rete e dei sistemi, sono obbligati a rispettare la totale riservatezza delle informazioni che incontrano.

Di conseguenza, non possono utilizzare né divulgare le informazioni alle quali hanno accesso in veste di Amministratori.

Si sottolinea che, in base alle normative sulla criminalità informatica, in caso di richiesta da parte dell'Autorità Giudiziaria, **ARS SERVICE S.R.L.** metterà prontamente a sua disposizione tutte le informazioni in suo possesso della natura richiesta mantenendo, come previsto dalla legge, totale riservatezza verso terzi sia dell'avvenuta richiesta sia delle informazioni messe a disposizione.

## **10. POLITICHE DI CLEAR DESK E CLEAR SCREEN**

Al fine di ridurre il rischio di accesso non autorizzato ad informazioni aziendali, è necessario che l'utente segua delle politiche di clear desk e di clear screen.

Con tali termini si intende che l'Utente presti particolare attenzione a materiale cartaceo, dispositivi di memoria rimovibili e schermate a video contenenti informazioni non pubbliche.

Di conseguenza, l'Utente dovrà aver cura di distruggere o immagazzinare in luoghi sicuri stampe, memorie di massa portatili e simili.

Particolare attenzione va posta alle stampe che, a volte, possono essere dimenticate sulle stampanti o ritirate dopo un tempo piuttosto lungo, lasciandole così incustodite e a disposizione di chiunque.

Anche le visualizzazioni a video possono contenere informazioni non pubbliche ed è quindi opportuno che tali schermate siano mantenute solo per il tempo strettamente necessario.

Anche l'utilizzo di riconoscitori vocali per la dettatura automatica deve seguire gli stessi principi.

## **11. INTEGRITÀ E DISPONIBILITÀ DEI DATI (CARTELLE DI RETE)**

L'integrità e la disponibilità dei dati aziendali è garantita dall'Amministratore di Sistema solo quando essi vengono trattati e memorizzati sui server di rete.

L'Utente è tenuto a trasferire tempestivamente e a mantenere nella propria cartella di rete i dati considerati importanti o critici per **ARS SERVICE S.R.L.** o per la propria funzione specifica, eventualmente presenti localmente sul proprio PC.

Resta pertanto inteso che eventuali dati memorizzati esclusivamente sulle postazioni di lavoro individuali non sono soggetti ad alcuna forma di protezione o salvataggio (backup) in caso di malfunzionamento, errore accidentale e/o manomissione.

## **12. UTILIZZO DEL PERSONAL COMPUTER**

Il personal computer (PC) utilizzato da ciascun lavoratore è uno strumento di lavoro.

Ogni suo utilizzo improprio può contribuire a creare disservizi, costi di manutenzione e soprattutto minacce alla sicurezza delle informazioni sensibili per il core business aziendale e all'immagine pubblica di **ARS SERVICE S.R.L.**

Ogni Dipendente/Collaboratore/Utente è pertanto responsabile dell'utilizzo e della custodia degli strumenti informatici ricevuti in dotazione.

Alla luce di ciò, a ciascun Dipendente/Collaboratore/Utente è fatto esplicito divieto di:

- modificare qualsiasi caratteristica hardware e software impostata sul proprio personal computer, salvo preventiva autorizzazione scritta da parte del Responsabile IT;
- installare e/o eseguire qualsiasi tipologia di programmi informatici diversi da quelli autorizzati dalla Società, anche nel caso in cui si tratti di software opportunamente licenziato, di software in prova (c.d. "shareware"), ovvero di software gratuito e liberamente scaricabile da Internet (c.d. "freeware");
- prelevare da Internet, copiare e/o archiviare sul personal computer qualsiasi genere d'informazioni (come, a mero titolo esemplificativo e non esaustivo, file audio, video, eseguibili, ecc.) non necessarie all'attività lavorativa;
- utilizzare qualsiasi tipologia di supporti di archiviazione removibile o di tecnologia di comunicazione per la memorizzazione o l'invio verso l'esterno di informazioni inerenti il rapporto di lavoro, se non a fronte di comprovate esigenze di servizio;
- lasciare incustodito e accessibile, ovvero cedere a soggetti non autorizzati il proprio personal computer, soprattutto successivamente al superamento della fase di autenticazione;

- eliminare la richiesta di password per il salvaschermo (screensaver) impostata automaticamente in caso di prolungata inattività da parte del lavoratore sulla sua postazione di lavoro, al fine di evitarne un utilizzo improprio in caso di assenza anche temporanea.

Fatte salve particolari esigenze tecniche o lavorative, le postazioni di lavoro devono essere spente al termine della giornata lavorativa.

L'Utente è responsabile del personal computer portatile eventualmente assegnatogli da **ARS SERVICE S.R.L.** e deve custodirlo pertanto con diligenza, sia durante gli spostamenti che nel corso del normale utilizzo.

Ai personal computer portatili si applicano tutte le regole di utilizzo e i divieti in precedenza previsti. In particolare, si ricorda che, a maggior ragione durante il loro utilizzo all'esterno delle nostre strutture, il computer portatile non deve mai essere lasciato incustodito e deve essere adeguatamente preservato nei luoghi e con i mezzi più idonei per la sua ottimale protezione.

Al suo interno inoltre devono essere immagazzinate le informazioni strettamente necessarie all'attività che si svolge al di fuori delle strutture aziendali, onde limitare la perdita di informazioni aziendali in caso di danno, smarrimento o furto.

In caso di furto o smarrimento, l'Utente assegnatario del personal computer ha l'obbligo d'informare tempestivamente il proprio diretto Responsabile e il Responsabile IT, nonché di denunciare tempestivamente l'accaduto alle Forze dell'Ordine, fornendo ad **ARS SERVICE S.R.L.** copia dell'atto di denuncia.

**ARS SERVICE S.R.L.** infine si riserva il diritto di controllare attraverso idonei sistemi tecnologici la coerenza dei programmi installati sul profilo utente del personal computer dato in dotazione.

Il Responsabile IT può, in qualunque momento e anche senza preavviso, procedere alla rimozione dell'applicazione che si dovesse ritenere pericolosa per la sicurezza del patrimonio informativo aziendale o che alteri la configurazione originaria della postazione di lavoro dell'Utente.

### **13. MODALITÀ DI ACCESSO ALLE POSTAZIONI DI LAVORO**

Tutti gli Utenti e i soggetti autorizzati che accedono agli archivi in rete devono essere accreditati tramite un codice identificativo.

Regole per la gestione dei codici di accesso:

- utilizzo di un codice univoco fornito e gestito dal Responsabile IT per ciascun Utente.
- Il codice è strettamente personale non cedibile.
- Uno stesso codice non può essere assegnato, neppure in tempi diversi, a persone diverse.
- In caso di non utilizzo per oltre sei mesi del codice di accesso lo stesso viene disattivato.

- La password deve avere una lunghezza di almeno 8 caratteri e non può contenere riferimenti personali che ne consentano un'agevole identificazione.
- La password deve essere modificata con una frequenza almeno semestrale.
- Il sistema tiene in memoria le ultime due password in modo che non possano essere replicate
- Il codice identificativo e la password devono essere custoditi con la massima diligenza e con il massimo grado di segretezza.
- Il Personale non può lasciare incustodita ed accessibile la propria postazione. A tal fine su ciascuna postazione deve essere configurato uno screen saver con password, che si aziona dopo 30 minuti di inattività.

#### **14. CONTINUITÀ DELL'ATTIVITÀ LAVORATIVA IN CASO DI ASSENZA DEL LAVORATORE/COLLABORATORE/UTENTE**

Nessuno può accedere alla postazione di lavoro elettronica utilizzando le credenziali di autenticazione di un altro Utente.

Un'eccezione a questa regola occorre solo nel caso in cui si verificano congiuntamente le seguenti condizioni:

- prolungata assenza o impedimento dell'Utente;
- l'intervento risulti essere indispensabile e indifferibile;
- vi siano concrete necessità di operatività e di garanzia della sicurezza del sistema.

A tale fine, in caso di prolungata assenza o impedimento, gli Utenti dovranno chiedere autorizzazione al Responsabile IT il quale fornirà una nuova password che dovrà essere utilizzata dall'Addetto per accedere al PC, avendo cura di cambiarla dopo il primo accesso.

Al ritorno dell'utente assente, lo stesso dovrà tempestivamente modificarla.

#### **15. UTILIZZO DELL'ELABORATORE E DELLA RETE INTERNA**

Nell'utilizzo del computer aziendale l'Utente deve osservare le seguenti regole:

- L'elaboratore e i relativi programmi e/o applicazioni affidati all'Utente sono strumenti di lavoro, pertanto:
  - vanno custoditi in modo appropriato;
  - possono essere utilizzati solo ai fini dell'esecuzione degli obblighi derivanti dal rapporto di lavoro/collaborazione, in relazione alle mansioni assegnate, e non anche per scopi personali o di qualsiasi altro tipo, anche se intrinsecamente non illeciti;
  - se ne deve segnalare all'Azienda il furto, danneggiamento o smarrimento.
- L'accesso al computer, sia esso in rete o stand alone, deve sempre essere protetto da una o più password; la password assegnata all'Utente non deve essere divulgata e deve essere custodita dall'assegnatario con la massima diligenza;

- Il monitor dei computer deve essere spento al termine della giornata lavorativa prima di lasciare gli uffici (salvo diverse disposizioni o in caso di particolare necessità); dovrà comunque essere attivato sul proprio computer uno screen saver con password;
- È espressamente vietato, in ogni caso, l'utilizzo di programmi per i quali non siano stati assolti tutti gli obblighi legati alla protezione della proprietà intellettuale imposti o richiesti dal titolare o dal legittimato allo sfruttamento economico, o che non siano distribuiti attraverso i canali ufficiali;
- Al fine di evitare i pericoli di contaminazione da virus informatici e/o di alterazione della stabilità delle applicazioni dell'elaboratore, è consentito installare programmi e software provenienti dall'esterno solo se espressamente autorizzati dal Responsabile IT;
- Non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- Non è consentito modificare le configurazioni impostate sul proprio computer o disattivare l'antivirus, se non previa autorizzazione dell'Amministratore di sistema;
- Non è consentita l'installazione sul proprio computer di mezzi di comunicazione propri (come ad esempio i modem);
- Sui computer dotati di scheda audio e/o di lettore CD o DVD o di altro dispositivo di lettura di supporti non è consentito l'ascolto o la visione di programmi, files audio-musicali o video, se non a fini prettamente lavorativi;
- Non è consentito scaricare files contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa;
- Tutti i files di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo e relativa autorizzazione all'utilizzo da parte dell'Amministratore di sistema. È inoltre vietato l'utilizzo di cd, DVD e di qualsiasi altro supporto di provenienza ignota;
- Le unità di rete sono aree di condivisione di informazioni strettamente aziendali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto è assolutamente vietata la dislocazione in queste unità, nemmeno per brevi periodi, di qualunque file o applicazione che non sia legato all'attività lavorativa. Il Responsabile IT si riserva la facoltà di procedere in qualunque momento alla rimozione, sia dagli elaboratori affidati o utilizzati agli Incaricati del trattamento dati sia dalle unità di rete, di ogni file o applicazione che riterrà pericolosi per la sicurezza del sistema e dei dati, che non sia inerente all'attività lavorativa ovvero che sia stato acquisito o installato in violazione delle presenti regole;
- L'Utente dovrà avere cura di mantenere negli archivi condivisi l'informazione aggiornata, rimuovendo e cancellando files obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente vietata una archiviazione ridondante che

non consenta in modo chiaro ed inequivocabile l'identificazione dello stato di revisione di un documento.

- L'Utente deve avere la cura di effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla immediatamente dal vassoio della stampante.

## **16. MODALITÀ DI GESTIONE DELLE PASSWORD**

### **a) Istruzioni per scegliere la password**

La password:

- non deve essere una parola ovvia quale:
  - nome proprio, nomi di animali
  - nomi di parenti, colleghi, superiori o dipendenti
  - nomi di città o nazioni, di strade, vie o piazze
  - l'identificativo utilizzato per la connessione al sistema (il cosiddetto ID User)
  - la propria data di nascita o altre date rilevanti
  - la targa dell'automobile
  - il proprio numero di telefono
  - il numero di matricola
- non deve essere una parola prevedibile quale:
  - un giorno della settimana, un mese
  - una password nuova che abbia una minima differenza con quella precedente (ad esempio l'ultima lettera diversa)
- non deve essere una parola comune nel gergo informatico quale ad esempio:
  - root, guest, password, computer, keyword, user, secret
- non deve essere lo stesso termine del codice identificativo, né un suo anagramma o il suo palindromo (ovvero la digitazione a rovescio)
- non deve essere una sequenza alfabetica o numerica, quali ad esempio:
  - abcdef, 123456, lmnopq, 987654
- non deve essere una sequenza di caratteri vicini tra loro sulla tastiera quali ad esempio:
  - qwerty, fred, pippo, asdfg, zxcvbn, poiuyt, mnbvcx
- devono contenere una combinazione di caratteri alfabetici, numerici o speciali, includendo in questi ultimi i segni di interpunzione e gli altri simboli resi disponibili.

### **b) Regole di conservazione della password**

Le password:

- devono essere custodite sempre con la massima riservatezza

- non devono mai essere rivelate a nessuno
- non devono essere annotate su carta né scritte altrove
- non devono essere mai riutilizzate né devono essere ripescate tra quelle vecchie, né devono assomigliare a quelle precedenti
- non devono essere quelle indicate a titolo di esempio dalla presente procedura e/o da manuali.

## 17. NAVIGAZIONE IN INTERNET

Internet è uno strumento messo a disposizione dell'Utente per uso professionale.

L'Utente deve quindi usare Internet e il browser in maniera appropriata tenendo presente che:

- L'accesso ad Internet è assegnato individualmente all'Utente per permettergli di visitare per uso professionale, sotto il nome di ARS SERVICE S.R.L., i siti disponibili. Tuttavia, è necessario considerare che quando si naviga nel Web, l'identificativo dell'Utente (che compare sotto il nome di ARS SERVICE S.R.L. sui siti esterni) ed i siti visitati vengono registrati entro i limiti della legge.
- Inoltre, ogni sito Internet può essere governato da leggi diverse da quelle vigenti in Italia; l'Utente deve quindi prendere ogni precauzione a tale riguardo.
- Tutte le azioni dell'Utente e tutti i dati riguardo all'Utente (siti visitati, messaggi scambiati, informazioni fornite tramite formati, dati raccolti all'insaputa dell'Utente, ecc.) possono essere registrati da chiunque all'esterno dell'Azienda e analizzati per determinare i suoi interessi, gli interessi dell'Azienda e usati per comunicati commerciali o per qualsiasi alta finalità. L'Utente a tale riguardo deve prendere tutte le precauzioni necessarie.

A scopo di statistiche, qualità del servizio e sicurezza, il traffico Internet può essere controllato e possono essere fatte da **ARS SERVICE S.R.L.** delle verifiche periodiche entro i limiti legali.

L'uso di Internet è consentito esclusivamente per scopi aziendali e pertanto non è consentito navigare in siti non attinenti allo svolgimento delle mansioni assegnate.

Non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi direttamente autorizzati dal proprio Responsabile gerarchico e con il rispetto delle normali procedure aziendali di acquisto.

Non è consentito scaricare software gratuiti (freeware e shareware) da siti Internet se non espressamente autorizzati dal Responsabile IT.

È vietata ogni forma di registrazione con dati identificativi aziendali (es.: e-mail @argussecurity.it, numero telefonico aziendale, indirizzo aziendale ecc.) se non esplicitamente autorizzati dal proprio Responsabile.

È vietata comunque ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

Non sono permesse, per motivi non professionali, la partecipazione a forum, l'utilizzo di chat line, di bacheche elettroniche, social network e simili, anche utilizzando pseudonimi (o nicknames).

Non è consentita la navigazione in siti e la memorizzazione di documenti informatici di natura oltraggiosa, pornografica e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

Tutti i file di provenienza incerta o esterna, anche se attinenti all'attività lavorativa, devono essere sottoposti al controllo antivirus.

Non è consentito scaricare e/o memorizzare file di grandi dimensioni; eventuali necessità attinenti all'attività lavorativa devono essere inoltrate al Responsabile IT.

Non è consentito l'invio di mail massive, ossia dirette ad un numero elevato di destinatari e con allegati di dimensioni significative, se non esplicitamente autorizzati dal Responsabile IT e solo per scopi lavorativi, nel rispetto delle politiche e delle norme sul trattamento dei dati personali.

Non è consentito connettere, neanche per breve tempo, gli strumenti informatici aziendali (personal computer, palmari, ecc.) a reti esterne pubbliche (Internet), private (sistemi di altre società) o reti domestiche per mezzo di collegamenti fisici con linee telefoniche, PSTN, ISDN, xDSL o con strumenti wireless di qualsiasi genere.

Da tale divieto sono da escludere gli accessi che avvengano tramite internet key e/o token di comunicazione aziendali.

Non è consentito l'utilizzo di connessioni wi-fi di qualsivoglia natura senza l'utilizzo di opportune precauzioni (token o cifratura).

Non è consentito lo scambio (ad esempio Peer-to-Peer) a qualsiasi titolo, anche se non a scopo di lucro, di materiale audiovisivo, cinematografico, fotografico, informatico, ecc., protetto da copyright.

Non è consentito l'utilizzo della connessione ad Internet e più in generale delle connessioni di rete disponibili, per tentare accessi a sistemi su cui non si è autorizzati.

È rigorosamente proibito qualsiasi uso del Web che non trasmetta un'immagine positiva di **ARS SERVICE S.R.L.** o che possa essere nocivo all'immagine di **ARS SERVICE S.R.L.**

Quindi, è proibita qualsiasi attività (di trasmissione / download / salvataggio / connessione) che può essere considerata come illegale, fraudolenta, spiacevole, di disturbo, offensiva, discriminatoria, diffamatoria, inclusa la connessione a siti pornografici oppure osceni.

Allo scopo di tutelare i propri sistemi informatici, **ARS SERVICE S.R.L.** adotta misure di protezione del traffico Internet anche mediante sistemi (surf control, firewall ecc.) finalizzati al blocco dell'accesso a determinati siti o contenuti. E' vietato aggirare o tentare di aggirare tali controlli (ad esempio mediante proxy anonimi).

## 18. USO DELLA POSTA ELETTRONICA AZIENDALE

La casella di posta elettronica assegnata da **ARS SERVICE S.R.L.** a ciascun Utente è uno strumento di lavoro.

Coloro i quali sono assegnatari di una o più indirizzi di posta elettronica sono responsabili del loro corretto utilizzo.

**ARS SERVICE S.R.L.**, pur proteggendo con gli opportuni software i sistemi di gestione delle caselle email da messaggi potenzialmente pericolosi, fa comunque esplicito divieto a tutti gli utenti di:

- utilizzare le caselle di posta elettronica aziendale ([nome.cognome@ars-altmann.it](mailto:nome.cognome@ars-altmann.it) oppure .de) per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list, ecc., salvo diversa ed esplicita autorizzazione;
- utilizzare le caselle di posta elettronica aziendale per l'invio di messaggi completamente estranei al rapporto di lavoro o alle interrelazioni lavorative tra colleghi;
- aprire email e/o gli allegati provenienti da mittenti sconosciuti o che abbiano anche solo un contenuto insolito; in caso di dubbio è fatto obbligo di avvisare preventivamente il Responsabile IT, che darà istruzioni in merito;
- inviare o dar corso a catene di messaggi.

**ARS SERVICE S.R.L.** fa obbligo a tutti gli utenti di:

- utilizzare le apposite funzionalità di sistema che, in caso di assenza (ad es., per ferie o attività di lavoro fuori sede), consentono di inviare automaticamente messaggi di risposta contenenti le “coordinate” (elettroniche e/o telefoniche) di un altro Lavoratore/Collaboratore/Utente, ovvero delle modalità utili a contattare **ARS SERVICE S.R.L.** Questo al fine di evitare e/o limitare il più possibile, in caso di necessità, l’apertura della posta elettronica del Lavoratore/Collaboratore/Utente;
- inserire all’interno dei messaggi di posta elettronica un avviso ai destinatari nel quale si dichiara l’eventuale natura non personale dei messaggi stessi e sia specificato se le risposte potranno essere conosciute nell’organizzazione di appartenenza del mittente.

La casella di posta elettronica, infine, deve essere mantenuta in ordine, archiviando documenti superflui, ridondanti o non “attivi” e, soprattutto, allegati ingombranti non più utili ai fini lavorativi.

Qualora il Lavoratore/Collaboratore/Utente, in deroga a quanto previsto nel presente paragrafo, utilizzi la casella di posta elettronica aziendale per fini privati e personali, i relativi messaggi devono essere immediatamente rimossi dalla cartella “Posta in arrivo” e “Posta inviata”, come pure dal “Cestino”.

Nel caso in cui il Lavoratore/Collaboratore/Utente ritenga di voler conservare questo genere di messaggi, deve provvedere ad archivarli in un'apposita cartella denominata "Personale".

La quantità di dati conservati in questa cartella non può comunque mai superare i 100 MB.

In caso di cessazione del rapporto di lavoro/collaborazione, per qualsivoglia ragione, il Lavoratore/Collaboratore/Utente, prima di lasciare il posto di lavoro, deve provvedere alla rimozione di detta cartella dal proprio personal computer aziendale, sia fisso che portatile. In mancanza sarà il Responsabile IT ad effettuare alla prima occasione utile questa operazione.

In caso di cessazione del rapporto di lavoro/collaborazione, per qualsivoglia ragione, il Responsabile IT provvederà ad effettuare copia e archiviare esclusivamente i messaggi di posta elettronica inerenti l'attività lavorativa.

Esaurite dette operazioni l'indirizzo di posta elettronica verrà disattivato.

#### **19. CONTINUITÀ NELL'USO DELLA CASELLA DI POSTA ELETTRONICA IN CASO DI ASSENZA DEL LAVORATORE**

In caso di eventuali assenze non programmate (ad es., per malattia), qualora il lavoratore non possa attivare la procedura in precedenza descritta e perdurando l'assenza oltre il limite temporale di 3 (tre) settimane, **ARS SERVICE S.R.L.** potrà disporre lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (ad es. il Responsabile IT oppure, se presente, un apposito Incaricato aziendale per la protezione dei dati), l'attivazione di un analogo accorgimento avvertendo precedentemente l'Interessato.

In previsione della possibilità che, in caso di ferie, assenza improvvisa ovvero prolungata, in caso di improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, il lavoratore verrà messo in grado di delegare un altro lavoratore fiduciario, preferibilmente operante nel medesimo settore del delegante, a verificare il contenuto di messaggi e a inoltrare al Titolare del trattamento dati quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.

Di tale attività verrà redatto a cura del Titolare del trattamento dati un apposito verbale e il lavoratore interessato verrà prontamente informato dell'accaduto alla prima occasione utile.

La delega perderà automaticamente la sua efficacia al rientro del Dipendente/Collaboratore/Utente.

#### **20. CONTINUITÀ NELL'USO DELLA CASELLA DI POSTA ELETTRONICA IN CASO DI FERIE DEL LAVORATORE DELEGATO**

In caso di ferie, qualora il periodo di assenza del lavoratore coincida in tutto o in parte con quello del delegato di cui al precedente paragrafo, il Dipendente/Collaboratore/Utente dovrà nominare un altro Collega fiduciario a conoscere il contenuto dei messaggi di posta elettronica e ad inoltrare al Titolare del trattamento dati quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.

Di tale attività verrà redatto a cura del Titolare del trattamento dati un apposito verbale e il lavoratore interessato verrà prontamente informato dell'accaduto alla prima occasione utile.

La delega perderà automaticamente la sua efficacia al rientro del Dipendente/Collaboratore/Utente.

## **21. PROTEZIONE ANTIVIRUS**

Ogni lavoratore deve tenere comportamenti atti alla cooperazione fattiva con **ARS SERVICE S.R.L.** per ridurre al minimo il rischio di attacchi ai sistemi informatici aziendali attraverso software malevolo (ad es., worm, virus, trojan, ecc.) e, più in generale, attraverso l'azione di programmi di cui all'art. 615- quinquies del codice penale, aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione totale o parziale, o l'alterazione del suo funzionamento.

Ogni utente, pertanto, è tenuto a:

- controllare la presenza e il regolare funzionamento del software antivirus installato;
- segnalare prontamente all'Amministratore del Sistema il caso in cui il software antivirus non riesca automaticamente ad eliminare la minaccia dai sistemi aziendali;
- verificare con il software antivirus, prima dell'apertura di qualsiasi file, ogni dispositivo (ad es., chiavette USB, DVD, CD, hard disk esterni, ecc.) proveniente dall'esterno della struttura e il cui utilizzo sia stato anteriormente autorizzato dall'Amministratore di sistema.

**ARS SERVICE S.R.L.** si riserva il diritto di installare su ogni postazione di lavoro elettronica i programmi che impediscano l'installazione e la diffusione di software potenzialmente dannosi per la sicurezza della rete aziendale.

La rimozione arbitraria di detti programmi è assolutamente vietata.

## **22. UTILIZZO DI APPARATI PER LA TELEFONIA MOBILE**

Ogni lavoratore che sia assegnatario di un telefono cellulare ovvero di qualsiasi dispositivo per la telefonia mobile, ivi comprese anche le sole schede SIM, ha l'obbligo di utilizzare detti strumenti esclusivamente per scopi intimamente connessi all'attività lavorativa e alle motivazioni che hanno spinto **ARS SERVICE S.R.L.** a fornire questa specifica dotazione.

Al fine di evitare qualsivoglia accesso e utilizzo indesiderato o illecito, è fatto obbligo che ciascun dispositivo venga protetto dal suo utilizzatore attraverso un codice PIN ovvero una parola chiave (password) che, nei limiti di quanto tecnicamente possibile, dovrà seguire le regole dettate in precedenza all'interno del paragrafo denominato "Modalità di gestione delle password".

Al momento della restituzione, l'Utilizzatore/Utente ha l'obbligo di cancellare qualsiasi informazione registrata all'interno del dispositivo, ivi compresi, a titolo esemplificativo e non esaustivo, nomi e cognomi, numeri di telefono, messaggi, fotografie, video e quant'altro sia conservato al suo interno. È fatto obbligo che ciascun dispositivo venga custodito con estrema diligenza. In caso di furto o smarrimento, l'Utente assegnatario del dispositivo ha l'obbligo d'informare tempestivamente il proprio diretto Responsabile e il Responsabile IT, nonché di denunciare tempestivamente l'accaduto alle Forze dell'Ordine, fornendo ad **ARS SERVICE S.R.L.** la copia dell'atto di denuncia.

### **23. UTILIZZO DI PC PORTATILI**

L'Utente è responsabile del PC portatile eventualmente assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo sul luogo di lavoro.

Al PC portatile si applicano le stesse regole di utilizzo previste per i PC fissi connessi in rete, con particolare attenzione alla rimozione di eventuali file che non devono essere salvati o archiviati.

I PC portatili utilizzati all'esterno (convegni, corsi, eventi vari etc...), in caso di allontanamento devono essere custoditi in un luogo protetto.

Il portatile non deve essere mai lasciato incustodito e sul disco devono essere conservati solo i files strettamente necessari.

Nel caso di accesso a Internet tramite la rete aziendale:

- Utilizzare l'accesso in forma esclusivamente personale;
- conservare la password in modo rigoroso;
- Disconnettersi dalla rete aziendale al termine della sessione lavoro.
- Collegarsi periodicamente alla rete interna per consentire l'aggiornamento dell'antivirus.

### **24. UTILIZZO DI SUPPORTI MAGNETICI**

L'utilizzo di supporti magnetici (cd, dvd, usb etc.) è consentito prestando la dovuta attenzione, custodendo con diligenza gli stessi e conservandoli nel rispetto delle misure di sicurezza in luogo sicuro ed accesso controllato.

Ai supporti magnetici si applicano le stesse regole di utilizzo previste per gli strumenti elettronici in quanto applicabili.

Ogni dispositivo magnetico di provenienza esterna dovrà essere verificato mediante sistema antivirus prima del suo utilizzo e, nel caso venga rilevato un virus dovrà essere consegnato al Responsabile IT.

Tutti i supporti magnetici riutilizzabili contenenti dati personali, in particolare se sensibili e/o giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato.

## **25. TELEASSISTENZA**

Relativamente all'attività di manutenzione remota su PC connessi alla rete aziendale il Personale esterno autorizzato potrà utilizzare specifici software.

Tali programmi vengono utilizzati per assistere l'Utente durante la normale attività informatica ovvero per svolgere manutenzione su applicativi e su hardware.

L'attività di assistenza e manutenzione avviene previa autorizzazione telefonica da parte dell'Utente interessato.

La configurazione del software prevede un indicatore visivo sul monitor dell'Utente che segnala quando il tecnico è connesso al PC.

Viene fornita, su richiesta, una comunicazione informativa sullo strumento utilizzato, nonché le modalità del suo utilizzo per tutti gli Utenti aziendali interessati.

## **26. MEMORIZZAZIONE FILE DI LOG DELLA NAVIGAZIONE INTERNET**

Al fine di verificare la funzionalità, la sicurezza del sistema e il suo corretto utilizzo, le apparecchiature di rete preposte al collegamento verso internet memorizzano un giornale (file di log) contenente le informazioni relative ai siti che i PC aziendali hanno visitato.

Tale archivio memorizza l'indirizzo fisico delle postazioni di lavoro e non i riferimenti dell'utente, garantendo in tal modo il suo anonimato.

L'accesso a questi dati è effettuato dall'Amministratore di sistema a ciò espressamente autorizzato anche sotto il profilo privacy.

I sistemi software sono programmati e configurati in modo da conservare per 48 ore i dati relativi agli accessi ad Internet e al traffico telematico.

L'eventuale prolungamento dei suddetti tempi di conservazione è eccezionale e può avere luogo solo in relazione ad esigenze tecniche o di sicurezza del tutto particolari, all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria oppure all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'Autorità Giudiziaria.

## **27. TRASMISSIONE E RIPRODUZIONE DEI DOCUMENTI**

Al fine di prevenire eventuali accessi ai dati aziendali da parte di soggetti terzi non autorizzati, occorre adottare delle cautele nella trasmissione e riproduzione dei documenti contenenti dati personali.

Quando il dato deve essere inviato a mezzo fax, posta elettronica, SMS, ecc. e, in particolar modo, nel caso in cui vengano inviati documenti contenenti dati sensibili occorre:

- prestare la massima attenzione affinché il numero telefonico o l'indirizzo e-mail immessi siano corretti;

- verificare che non vi siano inceppamenti di carta o che dalla macchina non siano presi più fogli e attendere sempre il rapporto di trasmissione per un'ulteriore verifica del numero del destinatario e della quantità di pagine inviate;
- nel caso di documenti inviati per posta elettronica accertarsi di avere allegato il file giusto;
- in caso di trasmissione di dati particolarmente delicati è opportuno anticipare l'invio chiamando il destinatario della comunicazione al fine di assicurare il ricevimento da parte del medesimo, evitando che terzi estranei o non autorizzati conoscano il contenuto della documentazione inviata.

Tutti coloro che provvedono alla duplicazione di documenti con stampanti, macchine fotocopiatrici o altre apparecchiature, in caso di copia da cui potrebbero essere desunti dati personali, sono tenuti a distruggere il documento mediante apposita macchina "distruggi documenti" o con qualunque altro mezzo che ne renda impossibile la ricostruzione in modo da escludere qualunque possibilità da parte di estranei di venire a conoscenza dei dati medesimi.

## **28. MISURE DI SICUREZZA PER IL TRATTAMENTO DI DATI PERSONALI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI**

Relativamente agli archivi cartacei valgono le seguenti regole:

- Il trattamento dei dati personali può essere effettuato solamente sulla base delle apposite autorizzazioni del titolare e, nel caso di dati sensibili, in conformità al consenso acquisito dagli interessati;
- Nessun soggetto esterno è autorizzato alla consultazione degli archivi cartacei, fatti salvi i casi previsti dalle norme di legge e per gli adempimenti statuari;
- Tutti gli archivi cartacei contenenti dati personali devono essere custoditi all'interno di appositi folder e riposti negli appositi armadi;
- Quando atti e documenti contenenti dati personali vengono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, tali atti e documenti devono essere controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e devono essere restituiti al termine delle operazioni richieste;
- L'accesso ai dati è consentito solo nei normali orari di lavoro ed è tassativamente vietato nelle altre ore della giornata;
- Non è consentita la riproduzione dei documenti cartacei se non agli Incaricati autorizzati;
- Il passaggio e la presenza di eventuali terzi presso gli uffici sono sorvegliati dal Personale aziendale, il quale fa in modo di evitare l'accesso ai vari uffici da parte di personale non autorizzato e/o non accompagnato da Personale aziendale.

## **29. MISURE DI SICUREZZA PER IL TRATTAMENTO DI DATI SENSIBILI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI**

L'accesso ai dati sensibili su supporto cartaceo è regolamentato, nel seguente modo:

- l'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative è soggetta ad aggiornamento periodico;
- Tutti i documenti relativi all'amministrazione del personale o contenenti dati sensibili devono essere custoditi negli appositi cassette o armadi dotati di chiavi. Le chiavi di accesso a tali cassette sono custodite in luogo non accessibile a terzi. Possono accedere a tali armadi solo i soggetti autorizzati. Il materiale prelevato deve essere trattenuto per il tempo strettamente necessario e conservato con le medesime modalità previste per l'archivio centralizzato.
- In alternativa dati sensibili, qualora disponibili in formato cartaceo, devono essere custoditi in armadi situati in un ufficio chiudibile a chiave;
- nessun trattamento di tali dati sensibili potrà essere effettuato se non sulla base delle apposite autorizzazioni del Titolare e/o del Responsabile e in conformità al consenso acquisito dagli interessati;
- gli Incaricati addetti dovranno negare l'accesso e la consultazione degli stessi archivi cartacei, fatti salvi i casi previsti dalle norme di legge e per gli adempimenti statutari;
- l'accesso selezionato agli archivi in cui vengono conservati atti e documenti contenenti tali dati dovrà esser fatto rispettare; nel caso in cui i documenti e gli atti in questione siano affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione e sono restituiti al termine delle operazioni affidate;
- l'accesso a tali dati è consentito solo nei normali orari di lavoro ed è tassativamente vietato nelle altre ore della giornata;
- L'accesso è in ogni caso controllato;
- Nelle ipotesi in cui dopo l'orario di chiusura siano ammesse persone a qualunque titolo, le stesse devono essere identificate e registrate.
- non è consentita la riproduzione dei documenti se non previa autorizzazione scritta del Titolare e/o del Responsabile.

## **30. MISURE DI SICUREZZA PER IL TRATTAMENTO DI DATI SENSIBILI CON L'AUSILIO DI STRUMENTI ELETTRONICI**

L'accesso ai dati sensibili gestiti in maniera elettronica è regolamentato nel seguente modo:

- il trattamento dei dati sensibili potrà essere svolto solo da Incaricati che abbiano ricevuto lettera d'incarico scritta da parte del Titolare e/o del Responsabile del trattamento;

- gli elaboratori utilizzati per il trattamento di dati sensibili non possono essere accessibili dalla rete pubblica ma devono risiedere su reti locali;
- ciascun incaricato del trattamento utilizza il proprio univoco codice di accesso per accedere ai sistemi; il codice per l'identificazione non può essere assegnato dal lavoratore ad altri incaricati, neppure in tempi diversi;
- la password d'accesso deve essere modificata con cadenza trimestrale;
- in relazione al trattamento dei dati sensibili, l'accesso da parte degli Incaricati del trattamento o della manutenzione deve essere espressamente autorizzato; le autorizzazioni vengono rilasciate e revocate dal Titolare e/o dal Responsabile del trattamento che con periodicità annuale verifica la permanenza delle condizioni per la loro conservazione.

I risultati della verifica annuale del permanere delle misure minime di sicurezza per la gestione dei dati personali e sensibili devono essere registrati su apposito Verbale di verifica;

- l'accesso ai dati sensibili per operazioni di manutenzione o trattamento dovrà in ogni caso essere limitato a quanto è indispensabile conoscere per effettuare tali operazioni;
- nel caso in cui siano impiegati, anche solo per aspetti particolari, soggetti esterni per l'adozione di misure minime di sicurezza, dovrà essere richiesta al soggetto esterno una descrizione scritta analitica dell'intervento effettuato che ne attesti la conformità alle disposizioni del Regolamento UE 2016/679 e della normativa vigente in materia di privacy.

### **31. DISTRUZIONE DOCUMENTI CARTACEI**

Tutti i documenti riportanti dati personali, dati sensibili e informazioni di tipo confidenziale devono essere distrutti utilizzando l'apposito distruggidocumenti messo a disposizione dall'azienda.

Il materiale cartaceo di scarto opportunamente distrutto deve essere smaltito in apposito sacco chiuso, onde evitarne l'accidentale fuoriuscita.

Il materiale cartaceo di scarto così trattato viene conferito al Servizio comunale di raccolta.

### **32. CONTROLLI E MONITORAGGIO DELLE RISORSE**

**ARS SERVICE S.R.L.** periodicamente o casualmente procederà, richiamate le garanzie della privacy previste, anche ad un controllo quantitativo dell'utilizzo della rete, dei PC e della posta elettronica per verificarne un uso equilibrato e coerente con l'attività aziendale.

In particolare, a titolo esemplificativo, controlli periodici potranno essere effettuati su:

- Il volume dei messaggi scambiati
- Il formato dei file allegati

- La durata dei collegamenti ad Internet
- I siti visitati più frequentemente
- Le informazioni raccolte dai dispositivi di sicurezza (Firewall, Antivirus, IDS, ecc.).

Tali controlli avverranno secondo il principio dell'incremento graduale del controllo.

In base a tale approccio, inizialmente i controlli vengono svolti su base aggregata e anonima.

Nel caso venissero riscontrati parametri anomali si potrà procedere all'individuazione delle aree interessate da tali anomalie ed effettuare comunicazioni specifiche a tale livello.

Se tali comunicazioni non dovessero portare ad una normalizzazione dei parametri misurati si potrà scendere, previo adeguato preavviso, a livello anche di singolo utente che, ove possibile, verrà invitato a partecipare direttamente alle attività di verifica.

Il monitoraggio non è finalizzato al controllo delle attività degli utenti (salvo eventuale esplicita richiesta in tal senso da parte delle Autorità competenti) ma solo al controllo dell'efficienza e dell'utilizzo corretto delle risorse informatiche aziendali e del network e si basa sul principio dell'incremento graduale del controllo stesso e, in generale, sul concetto di controllo difensivo ai sensi della legge.

I dati sopra descritti sono archiviati solo entro i limiti previsti dalla legge, salvo eventuale esplicita richiesta delle Autorità competenti.

In caso di attività sospette di gravità significativa queste potranno far scattare meccanismi di segnalazione all'Autorità Giudiziaria affinché avvii le indagini necessarie al fine di prevenire o sanzionare un reato, nell'ottica di tutelare gli interessi di **ARS SERVICE S.R.L.** e dei suoi Clienti e Fornitori.

**ARS SERVICE S.R.L.** si riserva il diritto di controllare con apposite attività ispettive il rispetto delle norme indicate nel presente documento.

Tali controlli saranno effettuati nella più stretta aderenza alle norme poste a salvaguardia della privacy dei dipendenti.

Tali attività saranno svolte per quanto possibile esaminando le registrazioni informatiche di sintesi, senza esame dei contenuti delle registrazioni e della posta elettronica, salvo quanto previsto precedentemente.

In ogni caso, ove siano necessari controlli che richiedano l'esame di contenuti, essi saranno condotti alla presenza dell'interessato, che potrà comunque impedire l'accesso ad informazioni da lui definite personali.

**ARS SERVICE S.R.L.** si riserva inoltre il diritto di procedere a controlli difensivi previsti dalla legge e comunque di mettere in atto tutto le misure per assicurare la gradualità dei controlli.

### **33. NON OSSERVANZA DELLA NORMATIVA AZIENDALE**

È fatto obbligo a tutti i Lavoratori/Collaboratori/Utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento.

Il mancato rispetto o la violazione delle regole sopra ricordate sono perseguibili nei confronti del Personale dipendente con i provvedimenti disciplinari previsti dal vigente CCNL, nonché con le azioni civili e penali consentite, mentre nei confronti del Personale non dipendente il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile con le azioni civili e penali consentite.

### **34. DENUNCIA AUTORITÀ GIUDIZIARIA**

Qualora comunque la tipologia, la quantità o la modalità di utilizzo improprio degli strumenti informatici siano tali da essere rilevanti ai fini del Codice Penale, **ARS SERVICE S.R.L.** provvederà obbligatoriamente ad effettuare specifica denuncia all’Autorità Giudiziaria.