VALORE CITTÀ AMCPS S.r.l.

REGOLAMENTO
PER L'UTILIZZO DEL
SISTEMA INFORMATICO AZIENDALE (SIA)

Approvato con Determina A.U. n. 57 del 3/07/2023

VALORE CITTÀ AMCPS S.r.l.

INDICE

1. PREMESSE 1

1.1. Entrata in vigore e pubblicità 1

2. CAMPO DI APPLICAZIONE DEL REGOLAMENTO 1

2.1. Oggetto e ambito di applicazione 1

2.2. Applicazione per il personale dell'Ufficio ICT 2

2.3. Sanzioni 3

3. LINEE GUIDA GENERALI 3

3.1 Titolarità, competenze e responsabilità 3

4. MISURE GENERALI DI SICUREZZA 5

5. L'ACCESSO AL SISTEMA INFORMATICO AZIENDALE 6

6. UTILIZZO DELL'HARDWARE 7

7. UTILIZZO DEI PROGRAMMI APPLICATIVI (SOFTWARE) 8

8. GESTIONE DEGLI ARCHIVI 10

9. RISERVATEZZA DELLE INFORMAZIONI 11

10. UTILIZZO DI INTERNET 12

11. UTILIZZO DELLA POSTA ELETTRONICA 13

12. PROTEZIONE ANTIVIRUS 15

13. ACCESSO AD ARCHIVI CONTENENTI DATI PERSONALI (REGOLAMENTO UE 679/2016 15

14. TUTELA DEL PATRIMONIO DELL'ENTE E RISPETTO DELLA RISERVATEZZA E DELLA DIGNITÀ DEL LAVORATORE 16

VALORE CITTÀ AMCPS S.r.l.

1. PREMESSE

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet dai Personal Computer espongono Valore Città AMCPS s.r.l. e gli Utenti (dipendenti e collaboratori della stessa) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e legge sulla *privacy*, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine della Società stessa.

Per questo motivo l'utilizzo delle risorse informatiche e telematiche aziendali, in applicazione di quanto disposto dagli artt. 2104 e 2105 c.c., deve avvenire nell'ambito del generale contesto di diligenza, fedeltà e correttezza che caratterizza il rapporto lavorativo fra Valore Città AMCPS s.r.l. e i lavoratori/Utenti, adottando tutte le cautele e le precauzioni necessarie per evitare le possibili conseguenze dannose che un utilizzo non accorto e consapevole di tali strumenti può produrre.

Il presente Regolamento è adottato al fine di richiamare le indicazioni e le misure necessarie e opportune per il corretto utilizzo nel rapporto di lavoro dei dispositivi elettronici aziendali in generale, degli archivi informatici, della posta elettronica e di Internet (nel loro complesso definito Sistema Informatico Aziendale), definendone le modalità di utilizzo nell'ambito dell'attività lavorativa e dando la massima diffusione alla cultura sulla sicurezza informatica.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli incaricati in attuazione del Regolamento UE 679/2016.

1.1. Entrata in vigore e pubblicità

Il Regolamento per l'utilizzo del Sistema Informatico Aziendale è stato introdotto per la prima volta nel 2003 da AIM Gruppo, di cui Valore Città AMCPS s.r.l. ha fatto parte dal 2010 e fino a fine del 2020. Da allora il documento è stato periodicamente aggiornato, pubblicato nella rete Intranet aziendale e affisso in bacheca. Gli aggiornamenti si rendono necessari in funzione dell'evoluzione normativa e tecnologica e sulla base delle nuove esigenze di sicurezza e di azioni correttive che si dovranno eventualmente intraprendere.

2. CAMPO DI APPLICAZIONE DEL REGOLAMENTO

2.1. Oggetto e ambito di applicazione

a) La Società utilizza sistemi informatici realizzati, gestiti o nella disponibilità di Valore Città AMCPS s.r.l. stessa.

b) Le informazioni formate, gestite e conservate da Valore Città AMCPS s.r.l. e i sistemi informatici a tale scopo utilizzati formano nel loro insieme il Sistema Informatico Aziendale (SIA). Tale Sistema è un patrimonio della Società. Il presente Regolamento contiene le disposizioni relative alle corrette modalità del suo utilizzo ed è compito di ogni collaboratore operare preservando e valorizzando questo patrimonio.

c) Il SIA è costituito dall'insieme degli strumenti tecnologici di cui la Società dispone per il trattamento delle informazioni, come *hardware* (personal computer, server di rete, stampanti e periferiche varie), *software* (programmi informatici di base e applicativi, database, ecc.) e reti telematiche, che sono messi a disposizione degli Utenti per permettere il quotidiano svolgimento delle proprie prestazioni lavorative.

   Fanno quindi parte del SIA anche tutti gli apparati removibili, i sistemi di identificazione e di autenticazione informatica, l'accesso ad Internet e gli strumenti di scambio di comunicazioni e *file*, la posta elettronica e, in generale, qualsiasi altro programma e apparecchiatura informatica destinata a generare, memorizzare e trasmettere dati e informazioni.

d) Il Regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori della Società a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratore a progetto, in stage, ecc.). Quindi, ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "Utente" deve intendersi il lavoratore in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata quale "incaricato del trattamento".

Per qualsiasi dubbio relativo all'applicazione pratica o all'interpretazione autentica delle disposizioni contenute nel presente Regolamento, è possibile rivolgersi al personale dell'Ufficio ICT (Information Communication Tecnology).

2.2. Applicazione per il personale dell'Ufficio ICT

Il personale incaricato, interno o esterno, che opera presso l'Ufficio ICT è autorizzato a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento, sostituzione, implementazione di programmi, manutenzione *hardware* etc.). La Società ha predisposto un canale informatico (GINWEB) unico e tracciato, per l'inoltro delle richieste di intervento tramite il quale gli utenti possono H24 effettuare tutte le richieste di intervento e di

supporto necessari alla corretta operatività.
Durante lo svolgimento di tali interventi, il personale incaricato dell'Ufficio ICT ha anche la facoltà di collegarsi e visualizzare in remoto i contenuti delle singole postazioni pc al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro *virus*, *spyware*, *malware*, etc. L'intervento viene effettuato esclusivamente su chiamata e autorizzazione dell'Utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

2.3. Sanzioni

In caso di accertata violazione da parte dell'Utente delle norme previste dal presente Regolamento, saranno applicate le sanzioni previste dai CCNL applicati al personale aziendale.

3. LINEE GUIDA GENERALI

La Società, consapevole delle potenzialità fornite dagli strumenti informatici e telematici, li mette a disposizione dell'Utente esclusivamente per finalità di tipo lavorativo. Non è quindi permesso utilizzare questi strumenti per altre finalità non connesse all'attività lavorativa o in modo che violino le leggi vigenti in materia.
Valore Città AMCPS s.r.l. potrà adottare accorgimenti tecnici necessari a tutelare la Società da eventuali comportamenti non permessi, salvaguardando il rispetto della libertà e della dignità dei lavoratori; gli eventuali trattamenti effettuati saranno ispirati a canoni di trasparenza.

3.1 Titolarità, competenze e responsabilità

Valore Città AMCPS s.r.l. è titolare di tutte le risorse *hardware* e *software* messe a disposizione degli Utenti del SIA.
L'*hardware* e il *software* in dotazione alle varie strutture è acquisito con il coordinamento dell'Ufficio servizio ICT sulla base delle specifiche tecniche da questo elaborate e messe a disposizione dei fornitori.
Tutte le risorse informatiche assegnate devono essere custodite con cura evitando ogni possibile forma di danneggiamento. Gli Utenti sono responsabili del corretto utilizzo degli strumenti messi loro a disposizione e della loro custodia e sono tenuti a segnalare tempestivamente dell'Ufficio ICT

eventuali guasti o difetti di funzionamento dei dispositivi *hardware* e *software*.

Il **Dirigente dell'Ufficio ICT** è tenuto a:

- elaborare le regole per un utilizzo ragionevolmente sicuro del Sistema Informatico della Società;
- implementare, con l'ausilio del personale dell'Ufficio ICT e/o di personale incaricato interno/esterno, le regole di sicurezza sul Sistema Informatico della Società assumendo il ruolo di "*custode*" delle credenziali di accesso ai sistemi informatici;
- monitorare il funzionamento dei sistemi del SIA, con l'ausilio di personale incaricato dell'Ufficio ICT e/o di personale incaricato interno/esterno, per individuare, nel rispetto della *privacy* degli Utenti, un eventuale uso degli stessi in contrasto con le disposizioni contenute nel presente Regolamento che possano compromettere le informazioni gestite nel SIA o esporre Valore Città AMCPS s.r.l. e gli Utenti a rischi di natura patrimoniale oltre che a responsabilità penali;
- attenersi alle prescrizioni previste nel Documento di adozione delle misure e accorgimenti prescritti dal Garante per la Protezione dei Dati Personali ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema.

I **Dirigenti e Responsabili di Valore Città AMCPS s.r.l.** sono tenuti a:

- applicare le disposizioni contenute nel presente Regolamento riguardanti le modalità di rilascio e revoca delle credenziali di autentificazione Utente;
- informare il personale dipendente e/o assimilato sulle disposizioni in merito all'uso consentito delle risorse del Sistema Informatico dell'Azienda;
- assicurare che il personale si uniformi alle regole e alle procedure descritte nel presente Regolamento;
- assicurare che i fornitori e/o il personale incaricato esterno si uniformino alle regole ed alle procedure descritte nel presente Regolamento;
- adempiere a tutti gli obblighi inerenti la responsabilità loro affidata in materia di trattamento di dati personali e sensibili gestiti dall'Azienda;
- segnalare prontamente al Dirigente dell'Ufficio ICT ogni eventuale attività non autorizzata sul SIA.

Il **personale dell'Ufficio ICT** ed il personale esterno incaricato che concorre alla gestione/implementazione del SIA è tenuto a:

- garantire la massima riservatezza sulle informazioni acquisite direttamente o indirettamente

nell'esercizio delle proprie funzioni;

- segnalare prontamente al Dirigente dell'Ufficio ICT ogni eventuale attività non autorizzata sul SIA.

Gli **Utenti del SIA** sono responsabili per ciò che concerne:

- il rispetto delle regole della Società per l'uso consentito del Sistema Informatico;
- l'uso delle credenziali di autenticazione loro assegnate secondo le modalità previste nel presente Regolamento;
- la pronta segnalazione al Dirigente dell'Ufficio ICT in merito a ogni eventuale attività non autorizzata sul SIA di cui vengano a conoscenza.

4. MISURE GENERALI DI SICUREZZA

a) Gli strumenti informatici possono essere utilizzati unicamente per gli scopi definiti dalla Società, utilizzando le procedure ed i programmi previsti e forniti dalla Società stessa. Pertanto, in linea generale non sono autorizzati gli utilizzi dei sistemi informatici che non sono previsti e specificamente definiti, come quelli per scopi personali.

b) Ogni Utente del Sistema Informatico Aziendale è tenuto ad osservare i comportamenti previsti dal presente Regolamento per garantire la massima sicurezza delle informazioni e l'integrità funzionale degli strumenti utilizzati.

c) Le componenti del Sistema Informatico Aziendale (*hardware, software,* reti) sono gestite unicamente dall'Ufficio ICT in forma diretta o tramite soggetti (imprese, consulenti, ecc.) che operano su incarico e per conto dell'Ufficio ICT. Nessun altro soggetto è autorizzato ad operare sul Sistema Informatico Aziendale.

d) Qualsiasi richiesta di intervento tecnico di qualsiasi natura a carico del Sistema Informatico Aziendale deve essere gestita dall'Ufficio ICT con personale interno o esterno. Non è permesso intervenire autonomamente o ricorrere in modo autonomo a prestazioni tecniche fornite da soggetti esterni.

e) È compito di ogni Utente evidenziare situazioni di utilizzo non autorizzato degli strumenti informatici e di riportare all'Ufficio ICT eventuali casi imprecisi o di difficile interpretazione.

f) È vietata l'installazione di programmi di qualsiasi genere o specie, se non dietro esplicita autorizzazione del Dirigente dell'Ufficio ICT.

g) Ogni Utente è tenuto a segnalare all'Ufficio ICT qualsiasi malfunzionamento degli strumenti informatici in uso.

h) Non è consentito procedere autonomamente a tentativi di correzione di errori o malfunzionamenti dei sistemi informatici, se non dietro esplicita autorizzazione e supervisione del personale dell'Ufficio ICT.

i) La configurazione dei personal computer della Società è realizzata su un modello standard appositamente studiato per garantire la semplicità di gestione del parco macchine e la condivisione delle risorse informatiche tra gli Utenti del Sistema Informatico Aziendale. Di conseguenza, non è permesso modificare la configurazione *hardware* del proprio posto di lavoro. In particolare, non è permesso spostare dispositivi quali unità centrali, unità video o stampanti, scanner, telefoni o fax, e installare o disinstallare dispositivi *hardware* (banchi di memoria, schede, *mouse*, stampanti, ecc.). Non è, inoltre, permesso modificare la configurazione *software* dei *personal computer*. In particolare, sono tassativamente vietate l'alterazione dei parametri di configurazione del sistema operativo, la modifica dell'interfaccia e comunque qualsiasi variazione alla configurazione originale *standard* prevista ed implementata su tutti i personal computer della Società.

j) Gli Utenti che, in seguito alla volontaria manomissione della propria postazione di lavoro, provocheranno la perdita di dati o comunque malfunzionamenti a carico delle apparecchiature, saranno ritenuti responsabili degli eventuali danni subiti dalla Società.

5. L'ACCESSO AL SISTEMA INFORMATICO AZIENDALE

a) L'accesso al Sistema Informatico Aziendale è consentito unicamente ai soggetti in possesso di credenziali personali di autenticazione rilasciate dall'Ufficio ICT. Per credenziale di autenticazione si intende l'insieme di identificativo Utente (UserID) e di parola chiave (*password*). Di norma l'identificativo Utente è composto dal nome e cognome dell'Utente separati dal simbolo "." (punto). Esempio: l'identificativo Utente di Mario Rossi è "mario.rossi".

   L'identificativo Utente è indispensabile per poter accedere al Sistema Informatico Aziendale. La UserID fornita all'avvio della sessione di lavoro permette al Sistema Informatico di riconoscere l'Utente e di consentirne l'accesso alle risorse informatiche per le quali è autorizzato (cartelle su *server* di rete, accesso ad archivi, accesso a programmi, Internet, posta elettronica, ecc.).

b) Le credenziali di autenticazione sono rilasciate individualmente e nominativamente a:

   - dipendenti di Valore Città AMCPS s.r.l. che nello svolgimento delle proprie mansioni

utilizzano il SIA;
- Amministratori della Società;
- consulenti e tecnici che, su incarico della Società e per lo svolgimento delle proprie attività, devono accedere al SIA;
- stagisti o personale a tempo determinato.

c) Le credenziali di autenticazione sono personali e devono essere utilizzate esclusivamente dal titolare. Il titolare provvederà a custodire e a garantire la segretezza della parola chiave e a sostituirla autonomamente almeno ogni sei mesi.

d) È assolutamente proibito accedere al SIA ed ai programmi con credenziali di autenticazione diverse da quelle assegnate.

e) Ciascun Dirigente o Responsabile è responsabile della gestione delle credenziali di autenticazione dei soggetti che operano all'interno della propria struttura (dipendenti, stagisti, consulenti, ecc.), in particolare della richiesta di nuove credenziali e di revoca di credenziali esistenti.

Le richieste di rilascio di nuove credenziali di autenticazione devono essere inoltrate in forma scritta al Dirigente dell'Ufficio ICT tramite il portale Richieste di intervento. Nella richiesta il Dirigente dovrà obbligatoriamente precisare a quali risorse informatiche l'Utente è abilitato ad accedere, come ad esempio archivi (*database*), programmi, cartelle residenti su *server* di rete, internet, posta elettronica, ecc.).

Anche le richieste di revoca di credenziali di autenticazione devono essere inoltrate in forma scritta al Dirigente dell'Ufficio ICT tramite il portale Richieste di intervento. La revoca deve essere richiesta nei seguenti casi:
- cessazione dal servizio o di trasferimento ad altra struttura di un dipendente;
- cessazione dal servizio di stagisti o di personale a tempo determinato;
- termine dell'incarico professionale assegnato a consulenti o tecnici esterni.

In caso di accesso indebito ad archivi aziendali effettuato con credenziali di soggetti non più in servizio e non revocate, il Dirigente dovrà rispondere degli eventuali danni arrecati alla Società e si esporrà alle sanzioni penali previste dal Regolamento UE 679/2016.

6. UTILIZZO DELL'*HARDWARE*

a) L'Ufficio ICT coordina l'acquisto delle apparecchiature informatiche necessarie per l'informatizzazione della Società. La tipologia, la dotazione e la configurazione delle

apparecchiature informatiche e dei posti di lavoro in generale sono definiti dall'Ufficio ICT sulla base delle esigenze degli Utenti e della integrazione e compatibilità col Sistema Informatico Aziendale.

b) L'installazione, configurazione e manutenzione di tutte le componenti del Sistema Informatico Aziendale sono gestite dall'Ufficio ICT.
c) È tassativamente vietato il collegamento al Sistema Informatico Aziendale di apparecchiature non di proprietà della Società o la connessione ad altre reti telematiche, salvo specifica autorizzazione dall'Ufficio ICT.
d) Tutti i dispositivi utilizzati dagli Utenti devono essere trattati con cura e deve essere segnalato qualsiasi malfunzionamento.
e) Non è autorizzato lo spostamento di alcuno strumento od accessorio fuori delle sedi aziendali, o tra sedi diverse, se non dopo esplicita autorizzazione da parte del Responsabile competente, sentito il parere del Dirigente dell'Ufficio ICT, fatta eccezione per le apparecchiature portatili (palmari, tablet, laptop).
f) Ogni Utente deve provvedere allo spegnimento dei dispositivi che ha in uso alla fine dell'orario lavorativo ed in tutti i casi di assenza prolungata dal proprio posto di lavoro, con esclusione delle postazioni che per ragioni di servizio devono rimanere sempre accese (es: *server* di rete). I dispositivi devono essere sempre spenti seguendo le procedure opportune (ad esempio, spegnimento mediante chiusura della sessione di lavoro in Windows).
g) È vietato lasciare incustodita la propria postazione informatica. In caso di temporanea assenza la propria postazione dovrà essere protetta attivando screen saver o la funzionalità "blocco PC".
h) Imballi e confezioni dei dispositivi in uso devono essere conservati o consegnati al personale dell'Ufficio ICT, salvo diverse disposizioni impartite dall'Ufficio ICT stesso. Manuali d'uso ed altri materiali di corredo dei dispositivi in uso devono essere conservati o consegnati al personale dell'Ufficio ICT, salvo diverse disposizioni impartite dall'Ufficio ICT stesso.
i) Licenze e documentazione di acquisto devono essere consegnate al personale dell'Ufficio ICT che ne cura la conservazione ai fini amministrativi e di controllo.
j) Gli Utenti non sono autorizzati ad operare su dispositivi di rete, quali *server*, stampanti condivise, dispositivi di connessione (prese di rete, *hub*, armadi di rete, *router*, stampanti di rete).

7. UTILIZZO DEI PROGRAMMI APPLICATIVI (*SOFTWARE*)

a) L'Ufficio ICT coordina l'acquisto delle licenze d'uso dei pacchetti applicativi necessari all'informatizzazione aziendale. Le caratteristiche del *software* applicativo acquistato sono definite dall'Ufficio ICT sulla base delle esigenze degli Utenti e della integrazione e compatibilità col Sistema Informatico Aziendale.
b) Le licenze d'uso dei pacchetti applicativi installati dall'Ufficio ICT sono di proprietà della Società.
c) I programmi applicativi sviluppati in proprio dalla Società attraverso i propri dipendenti o da terzi appositamente incaricati al fine di soddisfare esigenze di informatizzazione delle attività degli uffici rimangono di esclusiva proprietà della Società stessa.
d) L'utilizzo di tutti i programmi applicativi è limitato ai casi ed agli scopi previsti dalla Società. Non è comunque consentito l'utilizzo di programmi applicativi per scopi personali.
e) Non è consentito l'accesso a programmi od a parti di programmi applicativi cui non si è autorizzati anche se non esistono misure tecniche a protezione delle stesse.
f) Non è consentita l'esecuzione di alcuna modifica ai programmi applicativi se non, in casi particolari, dopo esplicita autorizzazione del Dirigente dell'Ufficio ICT. In particolare, non è consentita l'autonoma esecuzione di aggiornamenti, cambio di versioni o di lingua, spostamento di dischi o cartella di installazione, ad esclusione del personale dell'Ufficio ICT incaricato della gestione e manutenzione degli applicativi aziendali.
g) È vietata la duplicazione o copia parziale del software installato nel Sistema Informatico Aziendale, con esclusione delle copie di salvataggio effettuate dal personale del servizio ICT.
h) È vietata l'autonoma installazione di nuovi programmi applicativi, o di nuove versioni degli stessi. Ciò vale anche per le copie di software di cui l'Utente fosse venuto in possesso, ma anche per licenze gratuite (freeware) o per copie il cui possesso è legale (acquisto, regalo, prestito) ma non fa capo alla Società. Si precisa che l'inosservanza della presente disposizione espone la stessa Valore Città AMCPS s.r.l. a gravi responsabilità civili; si evidenzia, inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul software, che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate penalmente e possono anche comportare il sorgere di una responsabilità amministrativa a carico della Società, come disposta dall'art. 25–nonies del D. Lgs. 8 giugno 2001 n. 231, con applicazione di sanzioni pecuniarie ed interdittive.
i) L'Utente deve segnalare qualsiasi malfunzionamento od errore dei programmi applicativi in uso agli addetti dell'Ufficio ICT nei tempi più brevi; la segnalazione deve essere chiara e completa

e, se possibile, deve evidenziare le condizioni in cui si è verificato l'errore.

8. GESTIONE DEGLI ARCHIVI

a) Le informazioni generate dagli Utenti durante lo svolgimento delle proprie mansioni (documenti, archivi, dati in generale) costituiscono il patrimonio informativo aziendale e devono essere memorizzate unicamente sui dispositivi di rete (*server*) appositamente configurati dall'Ufficio ICT, salvo specifiche diverse disposizioni o per motivi legati alla conformazione della struttura della rete informatica.

b) Le attività volte a garantire la sicurezza delle informazioni memorizzate sui server di rete (es. le periodiche copie di salvataggio) vengono svolte dalle società esterne che si occupano della gestione dei server in cloud e della cybersecutity.

c) Sui sistemi aziendali di memorizzazione centralizzata (sistemi di storage) viene definita ed assegnata a ciascun Settore/Ufficio una specifica area (Quota disco) da utilizzarsi per la memorizzazione di files ed archivi; ciascun Utente potrà accedere solamente ai dati contenuti all'interno della cartella (e sottocartelle) dell'Azienda/Divisione/Ufficio di appartenenza, salvo eccezioni dettate da esigenze organizzative.

d) I singoli Utenti sono responsabili della integrità e riservatezza delle informazioni memorizzate sui server di rete nelle cartelle alle quali hanno accesso.

e) Le informazioni eventualmente memorizzate solo sui dischi locali dei computer non sono protette e non vengono incluse nelle copie di salvataggio. Gli Utenti saranno ritenuti responsabili della eventuale perdita o diffusione di dati di valenza aziendale memorizzati solo su dispositivi locali rispondendo dei danni subiti dalla Società.

f) Gli Utenti non sono autorizzati alla cancellazione di files o gruppi di files dei quali non conoscono scopo e/o contenuto. Gli Utenti hanno la facoltà unicamente di cancellare dai dispositivi in loro uso i files che hanno personalmente creato rispondendo degli eventuali danni subiti dalla Società.

g) Nel caso sia necessaria l'eliminazione di files per mancanza di spazio sui dischi di rete, tale operazione dovrà essere svolta con la supervisione degli addetti dell'Ufficio ICT.

h) Non è consentita la copia di archivi contenenti dati della Società di qualsiasi genere o specie su dispositivi asportabili (floppy disk, CD/DVD, USB pen drive, nastri e simili) né su dispositivi di memorizzazione esterni alla Società (ad esempio, in server accessibili mediante Internet) se non per attività istituzionali e dietro esplicita autorizzazione del Responsabile Aziendale del

Trattamento dei dati. In ogni caso, tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, etc.) contenenti dati sensibili nonché informazioni costituenti know–how aziendale, devono essere trattati con particolare cautela, onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

i) È vietato l'utilizzo di supporti rimovibili personali.

j) L'Utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.

k) L'Ufficio ICT, nell'ambito delle proprie attività di gestione e manutenzione del parco macchine, effettua controlli periodici sui personal computer in uso agli Utenti e in particolare sui dispositivi di memorizzazione locale. I programmi installati e le modifiche alla configurazione del PC non precedentemente autorizzati saranno cancellati ed il comportamento non autorizzato verrà segnalato al Dirigente di riferimento.

9. RISERVATEZZA DELLE INFORMAZIONI

a) Il Sistema Informatico Aziendale gestisce all'interno dei propri *database* dati personali così come definiti dal Regolamento UE 679/2016 sulla tutela dei dati personali. Ogni comportamento da parte degli utilizzatori del Sistema Informatico deve essere quindi conforme a quanto previsto dalla Legge e dai Regolamenti.

b) Ogni Utente ha accesso unicamente ai dati per i quali è stato autorizzato al trattamento. Questo si riferisce in generale a tutte le informazioni trattate dal Sistema Informatico Aziendale e, in particolare, ai dati personali, per i quali la Società assicura l'osservanza delle normative di legge.

c) Tutte le informazioni della Società sono riservate all'utilizzo ed alla circolazione unicamente all'interno della stessa, tranne nei casi diversi esplicitamente previsti. Nessuna informazione deve essere trattata, comunicata e diffusa all'esterno della Società se non nei casi previsti dalla Legge o dai Regolamenti.

d) È vietata la cifratura di documenti effettuata autonomamente dal dipendente se non in casi particolari e con l'autorizzazione del Dirigente di riferimento al quale deve comunque essere consegnata copia della chiave di cifratura.

e) Ai sensi del Regolamento UE 679/2016, il Titolare ed il Responsabile del Trattamento Dati possono richiedere al Dirigente dell'Ufficio ICT la disponibilità di dati o strumenti elettronici assegnati ad un dipendente in caso di sua prolungata assenza o di impedimento. Ciò avviene attraverso la sostituzione della password del dipendente effettuata dal Dirigente dell'Ufficio ICT

che la comunica al Titolare/Responsabile. Il Titolare/Responsabile che ha richiesto la sostituzione della password comunica tempestivamente e per iscritto al dipendente l'avvenuto cambio delle credenziali di accesso e le motivazioni.

10. UTILIZZO DI INTERNET

a) La Società mette a disposizione dei propri dipendenti l'utilizzo della navigazione Internet sulla base delle esigenze di ufficio e delle disposizioni del Dirigente di riferimento.
b) L'abilitazione per il dipendente all'utilizzo della navigazione Internet avviene all'atto dell'assunzione laddove necessaria per quanto al punto a).
c) È vietato l'utilizzo dell'accesso ad Internet per motivi personali.
d) La Società non è responsabile di eventuali dati personali, anche di tipo sensibile (es: cookies), che potrebbero risultare automaticamente memorizzati all'interno di postazioni di lavoro assegnate ad Utenti che, contravvenendo alla precedente disposizione, abbiano consultato siti per uso personale.
e) Non è consentito comunicare informazioni personali – anche se non riguardano la Società – nei siti visitati durante la navigazione, eccetto che per motivi strettamente legati alla propria attività e dopo esplicita autorizzazione del proprio Dirigente di riferimento.
f) È tassativamente vietato il download (memorizzazione sul disco del proprio computer o su altri dispositivi di memorizzazione, anche rimovibili) di files od archivi di qualsiasi genere trovati durante la navigazione su Internet, se non per motivi strettamente legati alla propria attività. In particolare, è vietato il *download* di contenuti protetti dalle leggi sul diritto d'autore (*software*, brani musicali, films, fotografie, ecc.)
g) Non è ammessa la partecipazione, per motivi non professionali, a Forum, Social Network, l'utilizzo di chat line o di bacheche elettroniche.
h) Non è ammessa la comunicazione di dati della Società in siti o sistemi di posta elettronica, se non dietro autorizzazione e per motivi direttamente collegati alla propria attività.
i) La Società adotta sistemi automatici di filtraggio degli indirizzi Internet (URL filtering) per impedire la navigazione all'interno di siti potenzialmente pericolosi per la sicurezza informatica del SIA.
j) La Società può avvalersi dei medesimi sistemi di cui al punto precedente anche per il trattamento di dati riguardanti il traffico Internet generato dalle stazioni di lavoro unicamente allo scopo di verificare ex–post comportamenti che abbiano causato danni alla Società, o per

controlli difensivi, oppure nell'ambito di indagini condotte dall'Autorità Giudiziaria. La raccolta e la custodia di questi dati sono effettuate nelle modalità previste dalla normativa vigente, in particolare dal Provvedimento 1° marzo 2007 *"Trattamento di dati personali relativo all'utilizzo di strumenti elettronici da parte dei lavoratori."* (GU n. 58 del 10–3–2007) e comunque con modalità tali da precludere l'immediata identificazione degli Utenti (es: mediante opportune aggregazioni).

k) Le informazioni di cui al punto precedente sono custodite per il periodo strettamente necessario legato all'indispensabilità del dato rispetto all'esercizio, alla difesa di un diritto in sede giudiziaria o a particolari esigenze tecniche o di sicurezza e poi sono distrutte.

l) L'accesso ai dati è consentito unicamente al Responsabile del Trattamento Dati e si effettuerà unicamente nei modi previsti dal Regolamento UE 679/2016 e, in particolare, secondo principi di gradualità dei controlli, pertinenza e non eccedenza.

m) I sistemi informatici di cui sopra non sono in alcun modo abilitati al "controllo a distanza del lavoratore".

11. UTILIZZO DELLA POSTA ELETTRONICA

a) La Società mette a disposizione dei propri dipendenti l'utilizzo di un sistema di posta elettronica sulla base delle esigenze di ufficio e delle disposizioni emanate in materia dagli Organi competenti.

b) Le caselle di posta elettronica sono di esclusiva proprietà di Valore Città AMCPS s.r.l.. Non è prevista la creazione di caselle e–mail per uso personale del dipendente e non è permesso l'utilizzo delle caselle di posta fornite dalla Società per motivi personali.

c) Le caselle possono essere intestate a Settori, uffici o singole unità operative. A queste potranno accedervi singoli dipendenti o gruppi di dipendenti a seconda delle esigenze organizzative. In caso di accesso consentito a gruppi di Utenti saranno generate singole credenziali per ciascun componente del gruppo. Tali credenziali dovranno essere custodite nei modi disciplinati dal presente Regolamento.

d) Le caselle possono essere intestate a singoli Utenti. L'assegnazione di una casella di posta elettronica con un indirizzo riportante il nome del dipendente non sottintende un uso personale della stessa, come evidenziato dal nome del dominio (amcps.it), e quindi la "personalità" dell'indirizzo non implica "privatezza" dello stesso.

e) I titolari di una casella di posta elettronica con un indirizzo riportante il proprio nominativo (es:

giovanni.bianchi@amcps.it) sono tenuti a riportare in calce alle proprie e–mail il testo predisposto dall'Ufficio ICT contenente un avvertimento ai destinatari nel quale sia dichiarata la natura non personale dei messaggi stessi, precisando che le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente.

f) La creazione di un nuovo indirizzo di posta elettronica deve essere richiesto dal Responsabile per iscritto all'Ufficio ICT utilizzando l'apposito portale Richieste di intervento, specificando il nominativo del dipendente cui è assegnato (referente).

g) Le caselle di posta elettronica devono essere di norma consultate ogni giorno. In caso di assenza prolungata del referente quest'ultimo dovrà utilizzare la funzionalità di "messaggio di risposta automatica per assenza" del sistema di posta.

h) È buona norma provvedere a eliminare periodicamente i messaggi più vecchi, ovvero a salvare su server di rete gli allegati per evitare la saturazione dello spazio della casella.

i) L'invio di messaggi che configurano impegni per la Società (come, ad esempio, ordini a fornitori, etc.) deve sempre seguire la procedura di approvazione prevista ed, in particolare, l'apposizione della segnatura di protocollo; non è permesso utilizzare il sistema di posta elettronica per modificare le procedure esistenti.

j) Ai sensi del Regolamento UE 679/2016 il Titolare ed il Responsabile del Trattamento Dati possono richiedere al Dirigente dell'Ufficio ICT la disponibilità della casella di posta elettronica assegnata ad un dipendente in caso di sua prolungata assenza o di impedimento. Ciò avviene attraverso la sostituzione della password del dipendente effettuata dal Dirigente dell'Ufficio ICT. Il Titolare/Responsabile che ha richiesto la sostituzione della password, comunicando tempestivamente e per iscritto al dipendente l'avvenuto cambio delle credenziali di accesso e le motivazioni.

k) Le caselle di posta elettronica assegnate nominativamente a dipendenti che cessano il rapporto di lavoro con la Società vengono disattivate al momento della cessazione dal Servizio su richiesta scritta tramite portale Richieste di intervento inviata dal Responsabile dell'Ufficio/Servizio cui apparteneva il dipendente cessato al Dirigente dell'Ufficio ICT. Per disattivazione si intende la disabilitazione della casella all'invio e alla ricezione di nuovi messaggi.

   La casella rimarrà disattivata per un periodo di dodici (12) mesi. Durante tale periodo la casella potrà essere consultata dal Responsabile dell'Ufficio/Servizio cui apparteneva il dipendente cessato, o da un suo delegato previa richiesta d'intervento indirizza al Dirigente dell'Ufficio

ICT tramite portale di Richieste di intervento. Terminato il periodo di disattivazione, la casella sarà rimossa dal *server* di posta.

12. PROTEZIONE ANTIVIRUS

a) Ogni Utente è tenuto a tenere comportamenti tali da ridurre il rischio di attacco al sistema Informatico Aziendale da parte di *virus* o di ogni altro *software* che operi con lo scopo di superare le difese di sicurezza del sistema stesso.

b) Nel caso in cui il *software antivirus* installato nel PC assegnato al dipendente rilevi la presenza di un *virus*, l'Utente dovrà immediatamente:
   - sospendere ogni elaborazione in corso senza spegnere il computer;
   - segnalare l'accaduto all'Amministratore del sistema.

c) Non è consentito l'utilizzo di dispositivi asportabili (*floppy disk*, CD/DVD, USB *pen drive*, nastri e simili) personali o comunque non provenienti dalla Società. Si consiglia di evitare la navigazione Internet su siti non istituzionali o la cui affidabilità non è accertabile. Si consiglia, inoltre, di non aprire files allegati ad e–mail provenienti da Utenti sconosciuti.

d) Ogni dispositivo magnetico o digitale di provenienza esterna alla Società dovrà essere verificato mediante il programma *antivirus* prima del suo utilizzo e, nel caso in cui venissero rilevati *virus*, dovrà essere consegnato al Dirigente dell'Ufficio ICT.

13. ACCESSO AD ARCHIVI CONTENENTI DATI PERSONALI (REGOLAMENTO UE 679/2016

a) La società, per perseguire le proprie finalità istituzionali, gestisce archivi contenenti dati personali tutelati dalla normativa in materia di *privacy*. A tal proposito, è stata nominata una specifica figura di Responsabile del Trattamento dei Dati.

b) L'accesso agli archivi contenenti dati personali (comuni e/o sensibili) è consentito esclusivamente agli Utenti autorizzati, detti anche Incaricati del Trattamento Dati. L'accesso viene consentito attraverso specifiche abilitazioni dell'Identificativo e della password dell'Utente.

c) Gli Incaricati del Trattamento dei Dati sono individuati e nominati direttamente dal Titolare del trattamento sulla base dell'analisi delle esigenze di servizio del Settore.

d) All'atto della nomina, gli Incaricati del Trattamento ricevono precise indicazioni sul tipo di trattamento dei dati che sarà loro consentito (lettura, modifica, cancellazione, stampa,

esportazione, importazione).

e) Nella gestione di archivi tutelati dalla normativa sulla *privacy* gli Incaricati dovranno attenersi a quanto previsto dal Titolare del Trattamento. In particolare, l'accesso ad archivi contenenti dati personali deve essere tassativamente circoscritto alle sole informazioni strettamente necessarie per adempiere ai compiti loro assegnati.

14. TUTELA DEL PATRIMONIO DELL'ENTE E RISPETTO DELLA RISERVATEZZA E DELLA DIGNITÀ DEL LAVORATORE

a) Le politiche della Società in materia di tutela del patrimonio aziendale e di rispetto della riservatezza e della dignità del lavoratore si ispirano alle Linee Guida del Gruppo di lavoro dei Garanti Europei ed applicano la normativa italiana e comunitaria.

b) Nella gestione del Sistema Informatico la Società opera ricercando un bilanciamento tra il diritto alla riservatezza dei lavoratori ed i propri legittimi interessi e, tra questi ultimi, il diritto di tutelarsi contro le responsabilità e i danni cui possono dare origine gli atti dei lavoratori. Tale bilanciamento è attuato in base a principi di proporzionalità e di trasparenza delle azioni e delle misure adottate nei confronti dei lavoratori. Altro principio guida è quello della prevenzione di atti o comportamenti illeciti e riguarda quelle azioni messe in atto dalla Società orientate a prevenire comportamenti illeciti che possono avere conseguenze dannose evitando così il ricorso a restrizioni drastiche nell'uso degli strumenti informatici o alla sorveglianza individuale e continuativa.

c) Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, Valore Città AMCPS s.r.l. può adottare eventuali misure che consentano la verifica di comportamenti anomali. A tal proposito i sistemi informatici aziendali e, in particolare, quelli preposti al trattamento dei dati personali o delle informazioni pubblicate su Internet, raccolgono informazioni tecniche riguardanti il funzionamento di tali sistemi. Tali informazioni sono utilizzate unicamente per la tutela del Sistema Informatico Aziendale al fine di identificare accessi e utilizzi illeciti ai sistemi ed alle informazioni e consentire l'adozione di adeguate misure di sicurezza informatica. L'implementazione di questi sistemi di monitoraggio è attuata in osservanza del Regolamento UE 679/2016 e alle specifiche tecniche internazionali in materia di sicurezza informatica (ISO 27000). Le finalità di tale trattamento sono pertanto connesse a specifiche esigenze organizzative, produttive e di sicurezza del lavoro, ma possono anche riguardare l'esercizio di un diritto in sede giudiziaria.

d) La custodia di tali informazioni tecniche è assicurata dal Responsabile del Trattamento Dati e, cioè, dal Dirigente dell'Ufficio ICT che previene qualsiasi accesso illecito a tali dati. A tal proposito sono adottate adeguate misure di sicurezza informatica.

e) In caso di accertate anomalie riguardanti l'utilizzo dei sistemi informatici, la Società tratterà le citate informazioni tecniche per effettuare controlli anonimi secondo principi di gradualità e proporzionalità su informazioni di tipo aggregato che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base individuale potranno essere compiuti solo in caso di ripetute successive ulteriori anomalie.

f) I controlli effettuati dalla Società utilizzando le informazioni di cui al punto precedente saranno attuati anche per la individuazione di accessi non autorizzati a sistemi ed informazioni o di comportamenti illeciti evidenziati dalla presenza nei sistemi informatici di *virus*, programmi *software* o altro materiale protetto da diritti d'autore privi di licenza d'uso. Le fattispecie oggetto di controllo difensivo sono quelle disciplinate dal Codice Penale in materia di reati informatici come, ad esempio: art. 420 c.p. *"Attentato ad impianti di pubblica utilità";* art. 615–*ter* "*Accesso abusivo ad un sistema informatico"*; art. 615 *quinquies "Diffusione di programmi diretti ad interrompere o a danneggiare un sistema informatico"*; art. 635–*bis "Danneggiamento di sistemi informatici e telematici"* e dagli artt. 2575 e seguenti del Codice Civile in materia di diritti d'autore.