REGOLAMENTO SULL'UTILIZZO DEGLI STRUMENTI INFORMATICI E DELLA RETE TELEMATICA

Sommario

CAPO I- OGGETTO - PRINCIPI GENERALI - AMMINISTRATORE DI SISTEMA

Art. 1 - Oggetto

1. Il presente disciplinare regola le modalità di accesso e l'utilizzo degli strumenti informatici e telefonici, dei software, delle banche dati e della rete internet ed il conseguente trattamento di dati personali nel rispetto di quanto disposto dal Decreto Legislativo 30 giugno 2003, n. 196 a seguito delle modifiche introdotte dal D.Lgs. 101/2018 (di seguito definito "Codice Privacy") e al "*Regolamento (UE) n.2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati"*(di seguito definito "GDPR"), ad integrazione delle regole derivanti dalla legislazione vigente, dalla contrattazione collettiva applicata,dal codice etico e dal codice di comportamento adottati da AFC Torino Spa e che in generale discendono dai principi di correttezza, diligenza e buona fede e di una condotta conforme ai civici doveri.
2. Il presente disciplinare definisce altresì le regole per il corretto utilizzo degli strumenti aziendali anche con riferimento all'installazione ed utilizzo di programmi ed applicazioni software garantendo al riguardo anche il rispetto delle disposizioni di cui alla L.633/41e s.m.i. nonché al D. Lgs.30/2005, relativi alla tutela del diritto d'autore,proprietà intellettuale ed industriale.
3. L'Amministrazione promuove ogni opportuna misura, organizzativa e tecnologica, volta a prevenire il rischio di utilizzi impropri delle strumentazioni e delle banche dati aziendali, al fine di evitare che, anche inconsapevolmente, possano minacciare oc compromettere la sicurezza del sistema informatico aziendale o la protezione dei dati ivi contenuti o arrecare un qualunque danno all'azienda (economico o di immagine).
4. Le presenti disposizioni si applicano a tutti gli utilizzatori interni ed esterni (amministratori, dipendenti dell'Ente o collaboratori, consulenti, stagisti, tirocinanti e soggetti autorizzati da AFC), che sono autorizzati all'utilizzo di dette risorse.

Art. 2 - Principi generali e pubblicità

1. AFC Torino Spa promuove l'utilizzo delle risorse informatiche hardware e software, della rete telefonica e telematica, di Internet e della Posta Elettronica quali strumenti utili a perseguire con efficacia ed efficienza le proprie finalità istituzionali, in accordo con le linee guida e i principi delineati dalla normativa vigente.
2. Ogni persona che ne fa uso è responsabile, civilmente e penalmente, del corretto uso delle risorse telefoniche ed informatiche, dei servizi/programmi a cui ha accesso e dei dati trattati a fini istituzionali. È altresì responsabile del contenuto delle comunicazioni effettuate e ricevute a fini istituzionali anche per quanto attiene la riservatezza dei dati ivi contenuti, la cui diffusione impropria potrebbe configurare violazione del segreto d'ufficio o della normativa per la tutela dei dati personali.
3. Sono vietati comportamenti che possano creare un danno, anche di immagine, ad AFC Torino Spa.
4. Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti. Il regolamento verrà diffuso al personale attraverso i canali telematici dell'Ente e distribuito nelle forme opportune a garantirne piena conoscenza.

Art. 3 - Amministratori di sistema

1. AFC Torino Spa aderisce al Consorzio CSI Piemonte, soggetto in house ed ente strumentale di tutti i consorziati ai quali eroga servizi in ambito informatico. In favore di AFC, il CSI Piemonte eroga servizi

infrastrutturali (quali i servizi di data center e infrastruttura di rete erogati in modalità hosting e cloud), servizi applicativi (sviluppati per la PA piemontese e/o ad hoc per AFC Torino, erogati in modalità SAAS); servizi di sicurezza, governo e sviluppo dei sistemi informativi aziendali.

2. Il CSI Piemonte è pertanto nominato Amministratore di Sistema ai sensi dell'art. 29 del GDPR. E' altresì amministratore di sistema il quadro aziendale assegnato ai Sistemi Informativi cui competono eventuali ulteriori specifiche deleghe di funzione nei confronti del personale assegnato al settore.
3. Chi amministra i sistemi è obbligato ad operare nel rispetto delle politiche dell'Ente in materia di sicurezza, a garantire la massima riservatezza nella trattazione dei dati personali anche desunti dal software di analisi del traffico, a mantenere riservate le informazioni relative al collegamento di chi utilizza i sistemi fatti salvi i casi di interessamento dell'Autorità Giudiziaria a fronte di ipotesi di reato.
4. I Sistemi Informativi possono revocare temporaneamente e in qualunque momento l'accesso alla risorsa telefonica o informatica e di rete, qualora queste siano utilizzate impropriamente o in violazione delle leggi vigenti. Potrà altresì interrompere temporaneamente la prestazione del servizio in presenza di motivati problemi di sicurezza, riservatezza o guasto tecnico, dandone tempestiva comunicazione a chi utilizza i sistemi.
5. I Sistemi Informativi possono accedere in qualsiasi momento, anche senza preavviso, ai locali e alle risorse informatiche dell'Ente, sia in caso di emergenza, sia per effettuare gli interventi di assistenza, verifica e supporto.

CAPO II - CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI

Art. 4 - Utilizzo del personal computer

1. Il personal computer (PC) è uno strumento di lavoro e il suo utilizzo deve essere finalizzato esclusivamente allo svolgimento delle attività professionali e istituzionali dell'Amministrazione. Il personal computer viene assegnato al personale dipendente, collaboratore o altra forma particolare di lavoro in relazione alle funzioni svolte. La collocazione del personal computer nella propria postazione di lavoro deve essere tale da ridurre il rischio di utilizzo a fini impropri e non legati all'attività lavorativa.
2. Ogni persona che utilizza i pc deve tenere comportamenti corretti, tali da preservare il buon funzionamento degli strumenti e tali da ridurre i rischi per la sicurezza del sistema informatico, ed evitare, salvo specifica e puntuale autorizzazione, l'utilizzo di supporti per la memorizzazione dei dati non sicuri e provenienti dall'esterno, al fine di non diffondere virus.
3. L'accesso alla postazione di lavoro è protetto da un sistema di autenticazione al dominio per l'accesso alla rete aziendale che richiede al lavoratore di inserire - all'accensione della propria postazione di lavoro - un codice utilizzatore (username) ed una parola chiave (password).
4. È necessario spegnere il personal computer al termine dell'attività lavorativa quotidiana.
5. Allontanandosi dalla propria postazione è opportuno bloccare temporaneamente la sessione di lavoro attraverso il comando CTRL+ALT+CANC→ Blocca oppure con TastoWindows + L per evitare accessi da parte di altre persone. La policy impostata di default blocca le sessioni di lavoro decorsi 15 minuti di inattività: l'utente può diminuire il tempo di inattività ma è fatto divieto di rimuovere il blocco.
6. Tutte le operazioni di login e logout dal dominio sono tracciate e i log (Ip, User, Timestamp) sono conservati per 6 mesi a fini di sicurezza interna, statistiche, prevenzione dei reati previsti dal modello organizzativo ex D.Lgs. 231/2001, trasmissione dei dati all'Autorità Giudiziaria in caso di formale richiesta e audit nel caso degli Amministratori di sistema.

7. E' fatto assoluto divieto di modificare le configurazioni hardware e software predefinite dagli amministratori di sistema ed installare autonomamente programmi o applicativi senza preventiva autorizzazione, come meglio specificato nel presente regolamento.
8. È vietata l'installazione non autorizzata di hardware che consenta l'accesso non controllato all'esterno della rete aziendale (ad es. internet key, chiavi Wireless USB o modem che sfruttino il sistema di comunicazione telefonico per l'accesso a internet o a banche dati esterne).
9. Sui dischi o altre unità di memorizzazione locale (es. disco C: interno PC) non vengono effettuate operazioni di salvataggio dei dati e non devono pertanto essere salvati i file aziendali, soprattutto se contengono dati personali: la responsabilità del salvataggio dei dati eventualmente ivi contenuti è pertanto a carico della singola persona che ne fa uso. In caso di infezione della postazione di lavoro e/o malfunzionamento quest'ultima potrà essere re-inizializzata con la relativa perdita di tutte le informazioni in essa conservate. In caso di necessità (anche solo temporanea) di mantenere per i fini di lavorazione una copia delle informazioni off-line (sul disco interno della postazione di lavoro), la copia locale deve essere eliminata al termine della lavorazione. I dati aziendali devono essere salvati all'interno delle aree operative, in base al settore di appartenenza: le unità di memorizzazione locale possono essere utilizzati solo in via transitoria.
10. Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
11. È vietato copiare o mettere a disposizione di altri soggetti materiale protetto dalla legge sul diritto di autore (documenti, files musicali, immagini, filmati e simili) di cui l'Ente non abbia acquisito preventivamente i diritti per la diffusione.
12. I sistemi Informativi possono procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza sia sui singoli personal computer sia sulle unità di rete, e possono, in qualsiasi momento, accedere al personal computer (anche con strumenti di supporto, assistenza e diagnostica remota) per manutenzione preventiva e correttiva, previa informazione alla persona interessata.
13. L'eventuale malfunzionamento o danneggiamento del personal computer deve essere tempestivamente comunicatoai Sistemi informativi.
14. È responsabilità del personale responsabile di ciascun servizio verificare il coerente utilizzo delle risorse assegnate al fine di prevenirne l'uso improprio o l'accesso alle risorse da parte di personale non autorizzato.
15. Nel caso in cui ci siano problemi sui personal computer, chi ne fa uso deve inoltrare apposita segnalazione, preferibilmente a mezzo mail utilizzando l'indirizzo sistemi.informativi@cimiteritorino.it o in alternativa a mezzo telefono, all'ufficio ICT (01101155330) - per richiedere l'intervento, indicandone il motivo.
16. Per la creazione di nuove utenze di dominio o per la loro cessazione, l'Ufficio del Personale comunica tempestivamente i dati anagrafici necessari (nome, cognome, codice fiscale) ed il settore di assegnazione/cessazione. Per l'allestimento di nuove postazioni o per lo spostamento di una o più PDL la persona Responsabile del settore è tenuta ad inviare una mail ai Sistemi Informativi, indicando la motivazione.
17. È vietato, in caso di cessazione del servizio, provvedere alla cancellazione dei file personalmente.

Art. 5 - Utilizzo delle unità di rete

1. Le unità di rete sono aree dedicate sui server aziendali per la condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. I Sistemi Informativi non rispondono dei dati personali eventualmente ivi custoditi in difformità alla

presente previsione.

2. Il personale che ne fa uso è responsabile per la protezione dei dati utilizzati e/o memorizzati nelle aree alle quali ha accesso; è fatto divieto di accedere direttamente o indirettamente a directory, files e servizi non pertinenti all'area di appartenenza qualora questo fosse tecnicamente possibile salvo siano espressamente e preventivamente a ciò autorizzati.
3. Sulle unità di rete, nel rispetto delle previsioni normative in tema di privacy e riservatezza dei dati, vengono svolte regolari attività di controllo, amministrazione e backup: i salvataggi periodici eseguiti con cadenza giornaliera consentono di ripristinare in toto oppure selettivamente eventuali files distrutti, per guasti hardware oppure per cancellazioni involontarie.
4. Le unità di rete finalizzate allo scambio di informazioni e alla scansione di documenti cartacei non sono destinate alla conservazione dei dati ed è fatto divieto di utilizzarle a tali fini: una volta acquisiti e salvati nell'area di destinazione i files devono essere prontamente rimossi a cura dell'utilizzatore.
5. I Sistemi Informativi provvedono a mantenerle in efficienza con periodiche cancellazioni dei dati: l'ufficio non risponderà di dati persi nell'ambito delle ordinarie attività di pulizia e manutenzione dello spazio disco.
6. I Sistemi Informativi possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno pericolosa per la sicurezza sia sui PC sia sulle unità di rete.
7. Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti da evitare un'archiviazione ridondante.
8. La cessazione di utilizzo di uno spazio disco (per cambio ruolo o responsabilità o organizzativo o cessazione del rapporto di lavoro) deve essere comunicata dalla persona gerarchicamente Responsabile della persona interessata ai Sistemi Informativi.
9. I Server sono ubicati presso la server farm del CSI Piemonte. Il CSI inoltre procede presso la sede di Vercelli ad una replica dei dati delle PA che supporta (Disaster Recovery). Nel caso residuale ed eventuale di server collocati in locali aziendali, l'accesso agli stessi è consentito al solo personale autorizzato espressamente dai Sistemi Informativi.

Art. 6 - Gestione delle password e degli account

1. L'account di accesso al personal computer e al dominio aziendale coincidono. E' costituito da un codice identificativo personale (username o user-ID) e da una parola chiave (password) assegnati da chi amministra i sistemi in fase di creazione utente. La password è valida soltanto per il primo accesso. I Sistemi Informativi comunicano la password solo alla persona interessata. Al primo accesso, il sistema richiede il cambio password.
2. Non è consentita l'attivazione nel BIOS dei personal computer della password d'accensione, senza preventiva autorizzazione da parte dei Sistemi Informativi.
3. La password dovrà essere costituita da almeno otto caratteri che possono essere lettere (maiuscole e/o minuscole), numeri e caratteri speciali, evitando contenuti di senso logico immediato facilmente individuabili e agevolmente riconducibili alla persona incaricata. La password non può contenere nome e/o cognome della persona interessata.
4. L'aggiornamento o il reset della password di dominio avviene attraverso la funzionalità messa a disposizione dal sistema operativo utilizzato (es. messaggio di avviso da parte del sistema operativo di scadenza e cambio attraverso la funzionalità "cambio password").
5. Anche tutti gli applicativi in uso prevedono l'utilizzo di una specifica password di accesso, i cui requisiti e le policy di aggiornamento dipendono dalle specifiche tecniche dell'applicativo stesso.

6. Se le credenziali sono state create dai servizi di assistenza, devono essere obbligatoriamente modificate al primo utilizzo, e mai salvate automaticamente per i successivi utilizzi delle applicazioni.
7. La password è personale e segreta: è cura di chi la utilizza, al primo accesso di qualsiasi programma – ove il sistema non lo richieda automaticamente - procedere alla modifica della parola chiave assegnata in fase iniziale. Ove non sia già impostata una scadenza temporale e automatica della password, la persona interessata deve provvedere almeno ogni tre mesi. Ove il sistema lo consenta, è vietato riutilizzare le ultime tre password utilizzate su quel programma.
8. Password, PIN e altre chiavi di accesso, devono essere custodite con attenzione e non devono essere riportate su fogli conservati sulle postazioni o nelle vicinanze.
9. La password non cedibile o trasmissibile ad altre persone: è fatto divieto di divulgare, password, username e comunque chiavi di accesso riservate. Se smarrite, va fatta immediata segnalazione e richiesta di sostituzione ai Sistemi Informativi.
10. È proibito entrare nella rete e nei programmi con nomi di utilizzo diversi dal proprio, fatto salvo quanto previsto al successivo comma;
11. In caso di assenze prolungate e programmate, qualora se ne ravvisi la necessità, la persona responsabile dell'ufficio cui è assegnato il/la dipendente, avvisato/a l'interessato/a, può richiedere ai Sistemi Informativi di accedere alla sua postazione ove siano stati salvati *files* in locale.
12. Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza o perché chi ne fa uso non la ricordi, i Sistemi Informativi procederanno alla sua riemissione, previa richiesta da parte della persona interessata.

Art. 7 - Utilizzo di computer portatili e tablet

1. I Sistemi Informativi assegnano computer portatili o tablet in relazione alla disponibilità e alla motivata richiesta formulata dalle Aree aziendali.
2. Chi utilizza l'apparecchiatura è responsabile del PC portatile eventualmente assegnato e deve custodirlo con diligenza sia durante glispostamenti sia durante l'utilizzo nel luogo di lavoro.
3. L'utilizzo dei personal computer portatili segue le stesse regole previste per i personal computer connessi inrete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna. E' fatto altresì divieto assoluto di modificare autonomamente la configurazione standard della postazione, sia sotto il profilo hardware che sotto il profilo software senza l'esplicita e documentabile autorizzazione della persona direttamente Responsabile.
4. I PC portatili utilizzati all'esterno (convegni, riunioni, ecc.), in caso di allontanamento, devono essere custoditi in un luogo protetto, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.
5. L'utilizzo della postazione mobile al di fuori della rete aziendale avviene esclusivamente tramite gli strumenti di accesso remoto sicuro profilati dai Sistemi Informativi quali il Remote Desktop System (RDS) e la Virtual Private Network (VPN). La connessione ad internet deve essere disposta mediante modem privato ovvero router mobile aziendale e/o smartphone aziendale o privato.
6. E' vietato memorizzare sull'hard disk dei computer portatili e/o dei tablet dati personali e/o dati aziendali.

   Tali strumenti dovranno essere sottoposti ad aggiornamenti dei sistemi operativi e delle applicazioni secondo le indicazioni che verranno fornite dai Sistemi Informativi
7. E' ammessa la fruizione dei dispositivi quali PC portatile, Smartphone e Tablet in ambito extra-lavorativo a condizione che l'uso dello strumento non comporti da parte del personale dipendente violazioni di norme di legge, regolamentazioni aziendali, danni economici e di sicurezza per l'azienda per i quali si considererà direttamente responsabile.

8. Non è invece consentito l'utilizzo di dispositivi personali quali tablet o pc portatili per le attività lavorative salvo le eccezioni autorizzate dai Sistemi Informativi, a condizione che l'uso del dispositivo personale non comporti da parte di chi ne fa uso violazioni di norme di legge, regolamentazioni aziendali, danni economici e di sicurezza per l'azienda, per i quali si considererà direttamente responsabile.

Art. 8 - Utilizzo dei supporti magnetici e dispositivi esterni; dispositivi di firma digitale

1. Non è consentito l'utilizzo né in lettura né in scrittura di dispositivi esterni personali (dispositivi di archiviazione USB, Schede SD, ecc.), salvo specifiche e puntuali deroghe.
2. In ogni caso non sono autorizzati dispositivi che contengano programmi eseguibili già preinstallati da utilizzare sulla propria postazione.
3. I dispositivi esterni aziendali (dispositivi di archiviazione USB, Schede SD, ecc.) possono essere utilizzati solo se in attinenza con la propria prestazione lavorativa e solo ove autorizzati per specifiche situazioni.
4. Tutti i supporti magnetici riutilizzabili (DVD, CD, dischetti, penne USB, hard disk esterni ecc.) che dovessero contenere 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 supporti magnetici contenenti dati sensibili devono essere custoditi in archivi chiusi a chiave. Ogni area aziendale è responsabile della custodia dei supporti ad essa assegnati e dei dati aziendali in essi contenuti.
5. La copia su supporti rimovibili di file contenenti dati personali o categorie particolari di dati, è da eseguire unicamente in via eccezionale e transitoria, deve essere crittografata e deve essere posta la massima attenzione alla conservazione del supporto cancellando i file appena possibile.
6. Non è consentito scaricare files contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa.
7. Tutti i files di provenienza incerta, ancorché potenzialmente attinenti all'attività lavorativa, non devono essere utilizzati/installati/testati. Nel caso di effettiva necessità di impiego devono essere sottoposti ad un preventivo controllo ed alla relativa autorizzazione all'utilizzo da parte dei Sistemi Informativi.
8. Tutti i supporti già contenenti dati aziendali ma destinati all'alienazione o a diverso utilizzo o a diversa persona, devono essere trattati in sicurezza, procedendo a seconda del caso con la formattazione o con la distruzione sicura, al fine di evitare che il loro contenuto possa essere recuperato dopo la cancellazione dei files da terzi non autorizzati. La distruzione sicura viene effettuata a cura dei Sistemi Informativi.
9. Ogni dispositivo magnetico di provenienza esterna all'Azienda, verrà automaticamente verificato dal programma antivirus nel momento in cui venga collegato al personal computer. Nel caso l'antivirus rilevi la presenza di un virus, il programma visualizzerà a chi ne fa uso un avviso di rilevazione virus e di spostamento automatico dello stesso in quarantena; si dovrà immediatamente segnalare la ricezione dell'avviso ai Sistemi Informativi. Contestualmente alla rilevazione, il programma antivirus procederà alla rimozione del virus dal dispositivo; ove non possibile l'antivirus ne inibirà l'utilizzo.
10. E' infine vietato costituire punti di accesso alle reti interne aziendali non controllati e autorizzati o utilizzare sistemi di cloudstorage per interscambio dati, diversi da quelli definiti dall'azienda. Per specifiche ed eccezionali esigenze di servizio, possono essere autorizzati sistemi esterni di condivisione dei dati.
11. Gli eventuali dispositivi di firma digitale in assegnazione, possono essere utilizzati esclusivamente per lo svolgimento dell'attività lavorativa.

Art. 9 - Utilizzo delle stampanti, delle multifunzioni e dei materiali di consumo

1. L'utilizzo delle stampanti e/o delle multifunzioni e dei materiali di consumo in genere (carta, inchiostro, toner, supporti magnetici, supporti digitali, ecc.) è riservato esclusivamente ai compiti di natura strettamente istituzionale. Devono essere evitati in ogni modo sprechi dei suddetti materiali e/o utilizzi eccessivi, avendo cura di stampare solo ove non sia agevole la lettura a video e di utilizzare prioritariamente il b/n, la funzionalità fronte/retro, la stampa di due o più pagine sulla stessa facciata.
2. Al fine di evitare trattamenti non consentiti di dati sensibili è vietato lasciare incustoditi presso le stampanti documenti cartacei contenenti dati sensibili.
3. A tal fine chi utilizza le stampanti deve usare la funzionalità di protezione di stampa sulle stampanti di rete (che permette di annullare il lancio di una stampa indesiderata ed evita distribuzioni non controllate di documenti).

Art. 10 - Utilizzo dei telefoni aziendali, fissi e mobili

1. I telefoni fissi o mobili assegnati, devono essere utilizzati, nell'ambito delle mansioni assegnate, per lo svolgimento dell'attività lavorativa.
2. Il personale identificato quale destinatario dell'apparato telefonico cellulare non può rifiutare l'assegnazione trattandosi di strumento di lavoro. L'apparato e tutti gli accessori con esso forniti dovranno essere conservati con cura e diligenza.
3. Nel caso di guasto dovuto ad incuria o di furto dell'apparecchio per negligenza, a chi ne fa uso potrà essere addebitato il 50% dell'importo eventualmente richiesto dal gestore telefonico ad AFC per la sostituzione dello stesso.
4. Per assicurare la sicurezza degli smartphone aziendali è previsto l'obbligo dell'autenticazione per l'accesso al dispositivo. All'accensione verrà richiesto obbligatoriamente l'inserimento di un codice, lasciando alla persona interessata la scelta di inserire una password, un PIN, un segno o il riconoscimento dell'impronta digitale o del viso. E' fatto divieto di disattivare tali sistemi di autenticazione anche ove l'apparato lo consentisse.
5. Il parco apparati è gestito centralmente dai Sistemi Informativi tramite il servizio MDM che consente la distribuzione controllata delle app, il ritrovamento di un cellulare perso o sottratto, l'inibizione dell'accesso ai contenuti non aziendali, la limitazione della navigazione in siti insicuri o inopportuni, la protezione degli apparati da attacchi esterni;
6. E' vietata in ogni caso l'attivazione dei servizi premium (sms e mms a pagamento) e le chiamate ai numeri che iniziano con l'89; tali servizi sono disabilitati e nel caso in cui, per motivi tecnici, fossero disponibili, ne è comunque vietato l'utilizzo. Gli eventuali costi derivanti dal precedente punto saranno oggetto di addebito diretto sullo stipendio.
7. Non è consentito l'utilizzo delle SIM aziendali su apparati personali perché questo potrebbe compromettere l'integrità della gestione dei dati aziendali;
8. Non è consentito l'utilizzo della SIM e dell'apparato aziendale per fini personali salvo episodici casi di forza maggiore da rappresentare prontamente al superiore;
9. Anche l'uso del telefono fisso per finalità personali deve considerarsi eccezionale e/o per urgenza e, di conseguenza, limitato a comunicazioni brevi ed a carattere puramente occasionale;
10. In ogni caso verranno disposti controlli al fine della corretta gestione della dotazione aziendale (si ricorda che, a tutela della privacy, nel dettaglio chiamate allegato al conto telefonico aziendale, non sono indicate le ultime tre cifre dei numeri chiamati dalle varie SIM) e l'eventuale traffico personale extra-canone verrà addebitato sullo stipendio.

11. Le SIM non sono abilitate al traffico in un paese extra UE. In ragione del ruolo aziendale, il traffico potrebbe essere temporaneamente abilitato previa specifica autorizzazione del Vertice aziendale.
12. Al personale quadro e alle figure impiegatizie apicali che ne facciano richiesta, ove l'apparato sia a tal fine predisposto, è concesso l'utilizzo della doppia SIM (personale e aziendale) previa configurazione di due partizioni a cura dei Sistemi Informativi.
13. Sulla partizione personale chi utilizza l'apparecchio può installare le app di suo interesse. La partizione aziendale rimane gestita dall'azienda. L'azienda non accede alla partizione personale.
14. I Sistemi Informativi, ai fini della verifica del corretto utilizzo, possono effettuare il controllo dei singoli apparati anche utilizzando le statistiche messe a disposizione dei sistemi di gestioni quali:
    a. quantità totale delle chiamate e dei messaggi scritti (SMS), classificata e misurata in termini percentuali sia in genere sia per la classe di destinatario, cioè in Rete Aziendale Mobile fuori della Rete stessa e per prefisso telefonico;
    b. durata e costo delle chiamate;
    c. orari di effettuazione delle chiamate.

Art. 11 - Software e copyright

1. Le dotazioni di software, standard e opzionali secondo le esigenze di servizio, sono gestite centralmente per tutti i dipendenti, ivi inclusi anche gli aggiornamenti.I Sistemi Informativi provvedono all'acquisto o alla regolarizzazione delle licenze necessarie per il software in uso presso l'Ente e mantengono aggiornato un "Catalogo del Software" in uso in azienda.
2. Al personale dipendente viene assegnato il profilo di "standard user", il quale non prevede la possibilità di operare in autonomia sulla propria postazione riguardo ad installazione software e aggiornamenti, salvo eccezioni esaminate singolarmente.
3. Il personale al quale sia assegnato il profilo di "Amministratore", che permette di operare in autonomia sulla propria postazione riguardo ad installazione software e aggiornamenti, deve operare nei limiti di quanto consentito dalle prescrizioni del presente regolamento.
4. Non è consentito l'uso di programmi diversi da quelli ufficialmente licenziati e/o in uso ad AFC ed installati dai Sistemi Informativi né è consentito a chi ne fa uso di installare autonomamente programmi provenienti dall'esterno, anche se memorizzati su dispositivi esterni quali chiavette usb e cd/dvd, sussistendo infatti il grave pericolo di introdurre Virus informatici, alterare la funzionalità delle applicazioni software esistenti, violare la normativa a tutela dei diritti d'autore sui software.
5. Sono inoltre vietate la duplicazione e qualsiasi forma di estensione d'uso del software aziendale, inteso sia come software prodotto direttamente dall'Azienda sia come software prodotto da terzi ed utilizzato dall'Azienda in forza di appositi contratti di licenza d'uso. Anche il software aziendale infatti è pienamente tutelato dalla normativa vigente in materia di proprietà intellettuale ed una sua duplicazione e/o un suo utilizzo non autorizzato o comunque difforme da quello definito nelle condizionidella licenza è vietato.
6. Le attività di testing di soluzioni reperibili in rete sono ammissibili al solo scopo di "testare", per un tempo limitato, la soluzione software e di verificarne l'eventuale utilità aziendale; le stesse devono essere effettuate nel pieno rispetto delle relative condizioni di licenza (in quanto versione "trial", etc.) e per il solo tempo strettamente necessario, decorso il quale vanno disinstallate.
7. E' anche vietato utilizzare servizi online anche gratuiti che i Sistemi Informativi non abbiano vagliato al fine della verifica delle condizioni di licenza.
8. È altresì vietata l'installazione di software o l'utilizzo di servizi on line non necessari per le attività

lavorative.

9. Qualora per lo svolgimento dell'attività lavorativa sia necessario un software non presente nel "Catalogo aziendale" o una versione diversa da quella disponibile, la persona interessata, attraverso la figura sua Responsabile dovrà comunicarlo ai Sistemi Informativi.
10. L'inosservanza delle presenti disposizioni espone la società a gravi responsabilità civili: 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 –rappresentano illeciti di rilievo penale.
11. È in ogni caso vietato:
    a. distribuire software soggetto a copyright acquistato da AFC Torino, al di fuori dei termini delle licenze;
    b. distribuire software che possa danneggiare le risorse informatiche, anche via e-mail;
    c. accedere a dati e/o programmi per i quali non vi è autorizzazione o esplicito consenso scritto da parte dell'intestatario.
12. L'utilizzatore risponde anche disciplinarmente del software installato sul computer in difformità da quanto indicato.
13. Tutte le postazioni e le configurazioni dei profili di chi utilizza i sistemi sono censiti centralmente in un apposito registro dedicato: i Sistemi Informativi attuano verifiche riguardo al software installato sui pc in dotazione (puntuali, periodiche e/o a campione), al fine di assicurare la conformità alla normativa in vigore e alle policy aziendali e alla rimozione del software non autorizzato.

CAPO III – CRITERI DI UTILIZZO DELLE RETI TELEMATICHE

Art. 12 - Gestione e utilizzo della posta elettronica e della posta elettronica certificata (pec)

1. Il dimensionamento della casella di posta è proporzionale alle funzioni svolte in azienda ed è governato dai Sistemi Informativi.

2. Il sistema di posta elettronica si compone inoltre di caselle di posta di gruppo alle quali ognuno, secondo l'appartenenza, accede con le proprie credenziali personali. L'utilizzo della casella di gruppo deve essere prioritario rispetto all'utilizzo della casella individuale là dove si tratti di comunicazioni di interesse condiviso.

3. Tutti gli indirizzi di posta sono consultabili direttamente dalla rubrica del sistema di posta in uso. Sono inoltre periodicamente aggiornati anche sulla rubrica aziendale disponibile sulla intranet.

4. Le persone a cui sono assegnati sono responsabili del corretto utilizzo della stessa: deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti al fine di evitare la saturazione della cassetta postale con conseguente impossibilità di utilizzo.

5. Il contenuto dei messaggi inviati deve essere espresso in maniera professionale e corretto e quindi non deve contenere espressioni che possano rivelarsi offensive, razziste, sessiste, discriminatorie o volgari.

6. Al fine dare informazione riguardo la natura esclusivamente aziendale della casella di posta elettronica, i messaggi devono contenere un avvertimento standardizzato nel quale sia dichiarata la natura non personale del messaggio, precisando che, il personale debitamente incaricato potrebbe accedere al

contenuto del messaggio inviato alla stessa casella. I sistemi Informativi provvedono a definire il messaggio standard da adottare e provvedono alla diffusione.

7. Per la trasmissione di categorie particolari di dati (personali sensibili e giudiziari), si raccomanda di prestare attenzione a che:

    a. L'indirizzo del destinatario sia stato correttamente digitato;
    b. L'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare la particolarità del dato;
    c. Gli allegati siano protetti con una password di accesso (comunicata con altro canale)

8. In caso di assenza programmata, utilizzare le funzionalità del sistema di posta per l'invio automatico di messaggi di risposta recanti le coordinate della casella di gruppo o della persona che sostituisce cui rivolgersi e la durata dell'assenza. In caso di assenze dal lavoro non programmate e prolungate, i Sistemi Informativi potrebbero procedere ad impostare di default l'inoltro sulla casella di un altro utilizzatore del medesimo gruppo di lavoro che verificherà il contenuto dei messaggi per processare quelli rilevanti ed urgenti.
9. Ai fini della sicurezza della rete aziendale, è necessario valutare l'affidabilità del mittente prima di accedere ai file allegati alla posta elettronica (non eseguire download di file eseguibili o documenti da siti Web o Ftp ambigui o comunque non conosciuti il cui indirizzo internet è inserito nel corpo della mail). Al fine di ridurre il rischio di diffusione di mail contenenti malware vengono applicati alla mail in ingresso filtri di controllo delle estensioni di allegati (es .zip, .rar .exe, etc) e filtri di limitazione anti-spam.
10. È fatto divieto di utilizzare la casella di posta elettronica per partecipazione a dibattiti, forum, o mailing-list e altre attività non attinenti la propria attività o funzione svolta per l'Ente, salvo diversa ed esplicita autorizzazione.
11. A titolo puramente esemplificativo, la persona che utilizza la posta elettronica non potrà usarla per:
    a. L'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es.mp3) non legati all'attività lavorativa;
    b. L'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list non coerenti con l'attività lavorativa;
    c. La partecipazione a catene telematiche (o di Sant'Antonio). Se si dovessero peraltro ricevere messaggi di tale tipo comunicarlo immediatamente ai Sistemi Informativi senza in alcun caso procedere all'apertura degli allegati di tali messaggi;
    d. L'iscrizione a newsletter salvo quelle utili alla propria attività in azienda.
12. Eventuali segnalazioni di mail ritenute sospette devono essere effettuateai Sistemi Informativi evitando di aprire gli allegati o i link riportati.
13. Non è consentito l'invio di messaggi con allegati di dimensione superiori a 10 Mb e con estensione uguali a .lnk .bat .exe .scr ed in generale file di tipo eseguibile o di applicazione. Per scambiare allegati che, anche dopo opportuna compressione, mantengano dimensioni superiori a tale soglia, occorre utilizzare strumenti di scambio documentale disponibili in internet e indicati ai Sistemi Informativi.
14. Il sistema di sicurezza e antivirus installato a protezione del server di posta elettronica di cui si avvale AFC Torino Spa potrebbe non consentire la ricezione e l'invio di messaggi di posta che contengono allegati con le caratteristiche sopra elencate.
15. È consentito l'accesso alla casella di posta elettronica individuale dall'esterno della rete LAN dell'Ente, anche mediante smartphone e/o tablet - aziendali o privati - nel rispetto delle norme di protezione dei dati personali.

16. Il personale del servizio ICT, nell'impossibilità di procedere come sopra indicato e nella necessità di non pregiudicare la necessaria tempestività ed efficacia dell'intervento, potrà accedere alla casella di posta elettronica per finalità di salvaguardia e sicurezza dei sistemi e/o nel caso le informazioni di pertinenza aziendale non siano altrimenti rinvenibili, procedendo a verbalizzare l'accesso, alla presenza di 2 persone incaricate, dando conto di motivazioni ed esito.
17. In caso di cessazione del rapporto di lavoro, l'indirizzo di posta elettronica individuale della persona interessata viene mantenuto attivo per un periodo di tempo pari a 6 (sei) mesi.
18. E' attivo il tracciamento e la conservazione dei log di posta per la durata di 12 mesi, per le seguenti finalità: per ragioni di sicurezza interna, statistiche, prevenzione dei reati previsti dal modello organizzativo ex D.Lgs. 231/2001, trasmissione dei dati all'Autorità Giudiziaria in caso di formale richiesta. I Backup delle caselle di posta vengono conservati per un periodo di 3 anni.
19. Per le comunicazioni ufficiali si raccomanda l'utilizzo della PEC aziendale esclusivamente per il tramite del sistema di Protocollazione e conservazione documentale adottato, sia in ricezione che in invio. Ove note, è fatto divieto di modificare le password di accesso alla casella di PEC aziendale per non compromettere la profilazione della stessa sul sistema di protocollazione.

Art. 13–LAN e Navigazione in Internet

1. L'azienda è dotata di una rete LAN Local area Network che consente la condivisione delle risorse informatiche e la navigazione in internet;
2. L'accesso alla rete LAN avviene attraverso le password di accesso al dominio (le stesse in uso per l'accesso al computer in dotazione);
3. E' vietato l'accesso alla rete LAN dall'esterno via modem o con qualsiasi altro mezzo di accesso remoto senza l'autorizzazione della figura responsabile della sicurezza informatica;
4. Il sistema informatico aziendale è protetto da software antivirus aggiornato quotidianamente. Ogni persona che ne fa uso deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale.
5. La navigazione in Internet è consentita per motivi strettamente legati all'attività lavorativa, fatta salva la possibilità di assolvere on line a piccole incombenze amministrative e burocratiche, come ad esempio l'effettuazione di adempimenti nei confronti di Pubbliche Amministrazioni e di concessionari di servizi pubblici, purché tale utilizzo sia limitato al tempo strettamente necessario, secondo quanto previsto nel regolamento Orario di Lavoro.

   A titolo puramente esemplificativo, il personale non potrà usare internet per:

   a. L'upload e/o il download di file del tipo MP3, AVI, MPG, e/o altri tipi di files o programmi per la fruizione di contenuto audio/video non legati ad un uso d'ufficio (ad esempio: film, musica e software);
   b. L'uso e la navigazione su siti non legati ad esigenze esclusivamente di tipo lavorativo, fatto salvo quanto previsto dall'art. 13 del Regolamento di disciplina dell'orario di Lavoro;
   c. Lo svolgimento di qualsiasi attività intesa ad eludere o ingannare i sistemi di controllo di accesso e/o sicurezza di qualsiasi server interno o pubblico, incluso il possesso o l'uso di strumenti o software intesi ad eludere schemi di protezione da copia abusiva del software, rivelare password, identificare eventuali vulnerabilità della sicurezza dei vari sistemi, decrittare file crittografati o compromettere la sicurezza della rete e internet in qualsiasi modo;
   d. L'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili non inerenti le proprie mansioni lavorative, fatto salvo quanto

previsto dall'art. 13 del Regolamento di disciplina dell'orario di Lavoro;

e. Ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa, fatto salvo quanto previsto dall'art. 13 del Regolamento di disciplina dell'orario di Lavoro;

f. La partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

6. Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa e operazioni quali l'upload o l'accesso a categorie di siti inseriti nella black list definita dall'azienda, ridurre gli usi impropri della navigazione in internet, prevenire eventuali controlli difensivi e per tutelare l'azienda ed i suoi rappresentanti da responsabilità anche penali connesse a reati commessi con modalità informatiche e telematiche, AFC ha adottato uno specifico sistema di blocco e/o filtro automatico (Proxy server), implementando le seguenti misure:
   a. Uso di filtri (URL Filtering e Content Filtering) che tracciano e prevengono determinate operazioni reputate inconferenti con l'attività lavorativa o ritenute a rischio per la sicurezza informatica (accesso a determinati siti inseriti in black list, e/o download di file o software);
   b. Uso di regole DLP (Data LossPrevention): al fine di tracciare e bloccare la diffusione di documenti marcati come riservati all'esterno del sistema informativo aziendale

7. La navigazione in rete deve quindi avvenire facendo rigorosamente uso dei dispositivi di protezione preposti quali sono i sistemi proxyed i firewall: sono pertanto vietati collegamenti personali derivanti da configurazioni non approvate che eludano tali sistemi di controllo (ad es. modem telefonici, linee adsl etc.).
8. In black list si trovano siti web non utili alla produttività dell'Ente e/o potenzialmente lesivi per l'infrastruttura, siti di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
9. I dati relativi alla navigazione bloccata dai sistemi di filtraggio (Data e ora della connessione; indirizzo di rete del PC; indirizzo di rete computer chiamato [server o generalmente host]) sono memorizzati tramite dispositivi elettronici e possono essere oggetto di controllo. Gli eventuali controlli, compiuti dai Sistemi Informativi avvengono mediante l'analisi dei "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre 6 mesi, in aderenza al principio di pertinenza temporale stabilito dal Codice sulla Privacy.
10. I dati di navigazione ed i contenuti dei siti internet consoni alle policy adottate non sono memorizzati dai sistemi di log.
11. Qualora tali sistemi di filtraggio impediscano l'utilizzo di siti o risorse utili all'attività lavorativa, la persona referente del servizio interessato a tale consultazione, deve inviare segnalazione via mail ai Sistemi Informativi.
12. L'utilizzo della rete internet resta assoggettato alle norme di Netiquette (insieme di regole che disciplinano il comportamento di un utilizzatore di Internet nel rapportarsi agli altri utilizzatori attraverso risorse quali newsgroup, mailing list, forum, blog o e-mail in genere).
13. Non è ammesso durante l'orario di lavoro, per esigenze non attinenti all'ambito lavorativo, l'utilizzo di chiavi personali con tecnologia GPRS, UMTS, HSDPA finalizzate alla ricezione di segnali tv o radio od alla navigazione incondizionata su internet.

Art. 14 - Piattaforme di Collaboration e Video-Conference

1. Le piattaforme di collaboration offrono strumenti per un supporto dell'attività lavorativa a distanza sia in tempo reale (es.videoconferenza, condivisione e modifica di documenti tra più persone nello stesso momento) che in modalità asincrona (es. uno spazio cloud per memorizzare condividere file).
2. Gli strumenti di collaboration, quando vengono impiegati per condividere documenti,video o immagini, devono essere utilizzati nel rispetto delle regole di comportamento suindicate al fine di garantire la riservatezza e in generale la sicurezza delle informazioni che possono transitare sulle stesse ma anche la tutela del segreto professionale, di marchi e del knowhow. In particolare, in relazione alla funzionalità di collaborazione in tempo reale è vietato effettuare snapshot o attivare la registrazione delle call al di fuori dei casi necessari ed espressamente autorizzati dai partecipanti (es. eventi di formazione).
3. E' vietata la conservazione permanente all'interno degli strumenti di collaboration, attraverso le funzioni di chat o in modalità asincrona (es. funzionalità di salvataggio file in OneDrive) di documenti contenenti dati personali per i quali è previsto esclusivamente l'utilizzo dei dischi di rete aziendali o dei database applicativi. Nell'ambito di attività temporanee di trattamento che richiedano l'interazione tra autorizzati tramite strumenti di collaboration, i dati personali devono essere crittografati ed eliminati al termine della sessione di lavoro.
4. E' consentito durante l'esecuzione delle call, l'uso della funzione di offuscamento dello sfondo o la disattivazione della telecamera. Le regole suindicate si applicano anche nel caso in cui vengano utilizzati strumenti di collaboration di uso comune quali come Skype, Zoom, Google Meet.

CAPO IV – PRIVACY, CONTROLLI E RESPONSABILITÀ

Art. 15 - la riservatezza dei dati gestiti con strumenti aziendali "non elettronici"

1. Per "non elettronici" si intendono sia documenti cartacei sia documenti di altro tipo come ad esempio microfilm, microfiches, lavagne e lucidi.
2. Per proteggere i dati personali o in genere riservati contenuti nei documenti è opportuno che essi non siano lasciati negli ambienti di transito o pubblici (corridoi o sale riunioni), o sulla scrivania ma siano riposti, quando non utilizzati e comunque al termine dell'attività lavorativa negli appositi archivi. Le stampe devono essere immediatamente ritirate dalle stampanti comuni. Eventuali supporti utilizzati in riunioni o corsi di formazione su cui siano stati riportati dati personali o riservati (es. lavagne) devono essere cancellati al termine dell'uso.
3. I documenti contenenti categorie particolari di dati devono essere custoditi in appositi armadi dotati di chiavi.
4. I locali ove sono presenti i documenti contenenti i dati personali (ed in particolare quelli di natura sensibile o confidenziale), devono essere soggetti a controllo e a verifica, al fine di evitare che durante l'orario di lavoro o al termine dello stesso possano essere conosciuti o accessibili da parte di soggetti non autorizzati. Si raccomanda, in caso di allontanamento dal proprio ufficio, di adottare tutte le accortezze e precauzioni al fine di impedire l'accesso fisico a chi non sia legittimato, soprattutto se esterno all'organizzazione di appartenenza.
5. Pertanto, le porte degli uffici ed almeno un armadio per ufficio devono essere dotati di serratura con chiave. Al termine dell'orario lavorativo, ove la dinamica delle attività ed il numero di persone occupanti lo consentano, è necessario chiudere sempre a chiave gli uffici nei quali vengono svolti trattamenti di dati personali.

6. I documenti cartacei ed i supporti removibili che contengono dati personali devono essere conservati esclusivamente per il tempo previsto nel piano di conservazione aziendale trascorso il quale devono essere distrutti (es. con un trita-documenti) e non gettati nei cestini.

Art. 16 - Controlli e responsabilità

1. AFC si riserva di effettuare controlli sul corretto utilizzo degli strumenti informatici, telematici e telefonici nel rispetto dei principi di pertinenza e non eccedenza, di correttezza e di gradualità come previsto dalla normativa vigente.
2. Per esigenze organizzative, produttive e di sicurezza AFC può avvalersi di strumenti che consentono un controllo a distanza di tipo generalizzato, indiretto e anonimo, relativo all'intera struttura amministrativa, ad aree, settori o gruppi di utilizzatore.
3. I controlli possono essere attivati dai Sistemi Informativi a seguito di richiesta della figura responsabile del servizio o a seguito della rilevazione di anomalie / malfunzionamenti del sistema. Il primo controllo sarà anonimo e nel rispetto del principio di gradualità. Qualora durante un controllo generalizzato vengano rilevate anomalie nell'utilizzo degli strumenti informatici, l'ufficio ICT procede preliminarmente all'invio di un avviso generalizzato relativo all'uso improprio riscontrato, con l'invito ad attenersi scrupolosamente al presente disciplinare, e riservandosi la facoltà di svolgere successive azioni mirate alla verifica del corretto utilizzo che saranno portate a conoscenza delle persone interessate e, se del caso, delle relative figure Responsabili, per eventuali precisazioni o contestazioni in merito.
4. Ove emergessero sospetti di reato le indagini saranno affidate all'autorità preposta.
5. Il personale incaricato che opera con funzioni di monitoraggio della sicurezza aziendale e di assistenza è autorizzato a compiere, nel sistema informatico aziendale, interventi tecnici e/o manutentivi diretti a garantire la sicurezza e la salvaguardia del sistema (es. attività di controllo, amministrazione e backup, ecc). Tali interventi, realizzati unicamente ai fini di garanzia della sicurezza ed estranei a qualsiasi finalità di controllo dell'attività lavorativa, possono anche comportare l'accesso ai dati trattati da ciascun lavoratore, ivi compresi: le mail di posta elettronica, i siti internet acceduti, i files dei dischi di rete e locali presenti negli archivi, file personali o programmi presenti sulla postazione di lavoro. In queste funzioni il personale incaricato è tenuto al segreto d'ufficio qualora venga in contatto con i dati personali ivi presenti.
6. Il monitoraggio dei sistemi informatici non rappresenta monitoraggio da remoto delle persone utilizzatrici.
7. L'azienda non usa software per monitorare il personale dipendente.
8. Il personale autorizzato può in qualunque momento procedere alla rimozione di file, applicazioni, software o altro che riterrà essere pericoloso per la sicurezza aziendale o in contrasto alle regole aziendali.
9. Il collegamento o la visualizzazione da remoto del desktop della singola postazione di lavoro, può avvenire solo previa esplicita segnalazione alla persona interessata, così anche per l'eventuale utilizzo della webcam.
10. E' inoltre prevista l'effettuazione di controlli atti a limitare la diffusione di malware all'interno della rete aziendale o altri problemi di sicurezza informatica. Per tali fini, in caso di evidenza di anomalia, vengono effettuate attività di verifica su alcune tipologie di log, tracciati dai sistemi di protezione, quali:
    a. I dati rilevati dalle console dei sistemi antivirus (numero infezioni, tipologia, pc infettati, user di appartenenza,etc.)

b. i log di posta e i log derivanti dalla applicazione dei mail filtering (caselle di destinazione/arrivo messaggi, ora/minuti invio/ricezione, tipologia di file allegato, user, ad esclusione dei contenuti della posta
c. i log dei sistemi di URL Filtering e Content Filtering (tracciatura delle URL permesse/bloccate dalle policy aziendali, tracciatura della connessione proveniente dagli IP/user, ora/minuto/secondo,server acceduto, pagina visitata, dimensioni file scaricato, numero di accessi continuativo)
d. i log DLP(analisi delle tracciature dei documenti riservati acceduti, ora/minuto/secondo, tipologia di regola di controllo,IP/user che ha effettuato l'azione)
e. i log di accesso ai data base od ai server aziendali.

11. A titolo meramente esemplificativo rientrano nella tipologia i controlli necessari a verificare:
    a. Le segnalazioni di frequenti e ripetuti tentativi di connessione provenienti dalle postazioni di lavoro verso siti i identificati come malevoli e pertanto bloccati, a partire da 20 connessioni/die
    b. le segnalazioni di tentativi continuativi provenienti dalla postazione conseguenti all'attuazione di blocchi della navigazione verso pagine di siti ritenuti a rischio per il loro contenuto, a partire da 20 connessioni/die
    c. gli accessi anomali (per frequenza o orario) da delle persone utilizzatrici, anche se autorizzati, a risorse di rete o documenti catalogati come riservati, a partire dalla singola connessione
12. Le anomalie riscontrate vengono verificate, quando possibile, con la persona interessata assegnataria della postazione al fine di identificare nel minor tempo possibile le cause che hanno portato alla generazione degli eventi potenzialmente malevoli e di intervenire per rimuoverne l'origine e bloccarne la diffusione.
13. Al fine di limitare e mitigare diffusione di virus e/o malware all'interno dell'azienda, sono presenti dei filtri di analisi di rete che sono in grado di analizzare eventuali connessioni o traffico di rete anomalo tra dispositivi interni o flussi sospetti dall'interno verso l'esterno.
14. E' inoltre possibile che per verificare il corretto utilizzo degli strumenti in dotazione vengano svolti controlli a campione mediante la raccolta e l'analisi di dati aggregati e anonimi. Nel caso di provato o constatato uso illecito o non consentito degli strumenti aziendali risultante dalla verifica delle informazioni in modalità aggregata e anonima, può essere necessario procedere alla verifica di mirate registrazioni delle sessioni di lavoro, al fine di verificare la correttezza dei comportamenti anche a fini disciplinari e al fine di fornire un riscontro all'eventuale richiesta dell'autorità giudiziaria, senza alcuna ulteriore informativa alla persona interessata.
15. Il periodo di conservazione dei log generati dagli strumenti di sicurezza sopra elencati non è superiore ai 6 mesi. Oltre alle finalità di sicurezza interna, i log vengono conservati per le seguenti finalità: statistiche, prevenzione dei reati previsti dal modello organizzativo ex D.Lgs. 231/2001, trasmissione dei dati all'Autorità Giudiziaria in caso di formale richiesta.

Art. 17- Responsabilità di chi utilizza i sistemi

1. Il personale dipendente deve attenersi, nell'utilizzo e nella gestione delle risorse strumentali informatiche aziendali, oltre che alle norme del presente disciplinare, ai principi e ai doveri stabiliti nel "Codice ETICO", alle prescrizioni contenute nel codice di comportamento e nel Modello di Gestione e Controllo adottato ai sensi del D.L 231/01.
2. Le persone che ne fanno uso sono tenute a mantenersi aggiornate, controllando periodicamente le direttive dei Sistemi Informativi divulgate tramite i canali telematici a disposizione dell'azienda;

3. La violazione da parte del personale dipendente dei principi e delle norme contenute nel presente disciplinare costituisce violazione degli obblighi e dei doveri del personale dipendente e pertanto, in relazione alla gravità dell'infrazione, previo espletamento di procedimento disciplinare, possono essere applicate le sanzioni previste dalle disposizioni contrattuali vigenti,
4. Tali violazioni possono inoltre costituire fatti penalmente o civilmente rilevanti.
5. Ogni utilizzo improprio delle risorse informatiche e/o telefoniche, ovvero mancanza di diligenza o comportamento doloso, causerà in capo al personale dipendente responsabilità per danno nei confronti azienda che promuoverà le azioni civili e penali consentite.

CAPO V - AGGIORNAMENTO E REVISIONE

Art. 18 - Revisione

1. Il presente regolamento è aggiornato in relazione all'evoluzione dei Sistemi Informativi e della normativa di riferimento. Tutte le persone che ne fanno uso possono proporre, quando ritenuto necessario, integrazioni alle presenti disposizioni. Le proposte verranno esaminate dai Sistemi Informativi.