Attività	Gestione Infrastrutture e sistemi informativi
Codice	A103-RG001
Titolo	**Regolamento per l'utilizzo degli strumenti informatici, della posta elettronica e della rete internet, nonché per la disciplina dei controlli nella ATS della Città Metropolitana Milano.**
Revisione	01 Data 23/09/2020
In vigore	dalla data di deliberazione

Distribuzione controllata in formato elettronico. L'originale firmato è agli atti presso *l'UOC Attività Istituzionale e di Controllo*

Gruppo di Lavoro che ha collaborato alla redazione del documento: //

Redazione

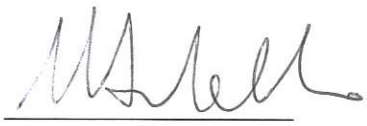
Dir. UOC Sistemi Informativi Aziendali
Veronica Monaci
Dir. UOC Risorse Umane e Organizzazione
Paola Carini
Dir. UOC Attività Istituzionale e di Controllo
Giovanni Cialone

Verifica

Dir. Amministrativo
Giuseppe Micale

Verifica conformità al SGQ

Resp. UOS Standard di Qualità
Mariangela Autelitano



Approvazione

Dir. Generale
Walter Bergamaschi

Indice

Causale di redazione

Tabella revisioni

Rev00	Prima emissione
Rev01	Inserimento articoli relativi a sistemi di archiviazione online (es.: Sharepoint) e smart working.

ART. 1 OGGETTO E FINALITÀ

1. Il presente Regolamento è redatto:

- alla luce della Legge 20/5/1970, n. 300, recante "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento";
- ai sensi della Direttiva del 26 maggio 2009 n. 02 del Ministero per la Pubblica Amministrazione e l'Innovazione: "Utilizzo di Internet e della casella di posta elettronica istituzionale sul luogo di lavoro";
- ai sensi del Provvedimento del Garante per la protezione dei dati personali, del 01 marzo 2007, recante "Lavoro: le linee guida del Garante per posta elettronica e Internet";
- vista la Raccomandazione CM/Rec (2015) del Comitato dei Ministri degli Stati Membri sul trattamento di dati personali nel contesto occupazionale;
- richiamato il Regolamento UE n. 2016/679 - in data 27 aprile 2016 - relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
- in attuazione del Decreto Legislativo n. 196 del 23 giugno 2003 – come modificato dal Dlgs 101/2018 -, recante "Codice in materia di protezione dei dati personali";
- ai sensi del Codice di comportamento di ATS della Città Metropolitana di Milano.

2. La finalità è quella di garantire il corretto utilizzo, nel rapporto di lavoro, degli strumenti informatici, della posta elettronica e della rete Internet a tutela della riservatezza dei dati, delle funzioni pubbliche d'istituto, dei principi e disposizioni di cui al codice di comportamento/disciplinare, di attuazione del disposto costituzionale di cui all'Art. 97 - per il buon funzionamento e andamento della Pubblica Amministrazione -. A tal fine, sono altresì regolate le modalità con le quali l'ATS della Città Metropolitana di Milano (di seguito ATS) può accertare ed inibire le condotte illecite degli utilizzatori di Internet, della posta elettronica e dell'accesso alle risorse di archiviazione di massa (server – hard disk).

3. Sono destinatari del presente regolamento i dipendenti, i collaboratori, gli stagisti, borsisti, i lavoratori interinali che utilizzano per la loro attività strumenti informatici, della posta elettronica e della rete Internet di ATS.

ART. 2 PRINCIPI GENERALI

1. I principi che sono a fondamento del presente Regolamento sono gli stessi espressi nel D.Lgs. 196/03, e, precisamente:

a) il principio di necessità per il quale: l'utilizzo dei dati personali, attraverso l'impiego di sistemi informativi e di programmi informatici, deve essere ridotto al minimo tenuto conto delle finalità perseguite;

b) il principio di correttezza, per il quale: le caratteristiche essenziali dei trattamenti, siano essi svolti in modalità cartacea od informatica oppure mista: cartacea ed informatica, devono essere partecipate ai lavoratori;

c) le finalità alla base del trattamento dei dati personali devono essere: determinate, esplicite e legittime, oltre che pertinenti e non eccedenti.

2. È riconosciuto all'ATS, in quanto datore di lavoro, il potere/dovere di svolgere attività di monitoraggio, che nella fattispecie saranno svolte:

- dal Direttore della UOC Sistemi Informativi Aziendali;
- dagli Amministratori di Sistema e/o dal personale delegato dal Direttore della UOC Sistemi Informativi Aziendali;

fatto salvo quanto disposto dall'art. 10 del presente Regolamento.

ART. 3 TUTELA DEL LAVORATORE

1. In ottemperanza all'art. 4, comma 1, L. 300/1970, la regolamentazione della materia indicata nell'Art. 1 del presente Regolamento, non è finalizzata all'esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro, risultando finalizzata all'uso dei sistemi e prodotti informativi da parte del lavoratore nel rispetto delle esigenze produttive ed organizzative nonché nel rispetto della sicurezza nel trattamento dei dati personali e delle informazioni.

2. È garantito al singolo lavoratore il diritto di accesso ai documenti personali che lo riguardano, nei modi stabiliti dal Regolamento sull'esercizio del diritto di accesso ai dati personali trattati dall'ATS, ai sensi del Capo V della L. 241/1990 e s.m.i. nonché di accesso ai dati nei modi di cui agli artt. 7 e 8 del D.lgs. 196/2003 e all'art. 15 del Regolamento UE 2016/679 in materia di trattamento dei dati personali (privacy).

ART. 4 ACCESSO A INTERNET E USO DELLA RETE AZIENDALE

1. L'accesso alla rete informatica e telematica aziendale è protetto da credenziali di autenticazione (username e password); le credenziali di autenticazione sono strettamente personali e identificano l'utente che accede ed utilizza la rete aziendale e/o effettua l'accesso ad Internet. È fatto divieto di comunicare ad altri soggetti, diffondere o rendere in qualsiasi modo pubbliche le proprie credenziali di autenticazione. L'utente è tenuto a custodire le proprie credenziali nella massima segretezza. Si rinvia ad apposita procedura aziendale per quanto riguarda le modalità di assegnazione di username e password, del primo accesso e della revoca (A103-Pd002 e smi).

2. Per rafforzare la sicurezza delle credenziali è disponibile, per i principali servizi di rete di ATS (es. posta elettronica, Onedrive, Sharepoint Online, etc.), il meccanismo di autenticazione a più fattori (multifactor authentication) che consiste nell'utilizzare - oltre alla coppia nominativo/password - un ulteriore fattore di autenticazione come ad esempio un'applicazione cellulare o l'invio di un codice tramite telefono o messaggio. Gli utenti potranno configurare tale soluzione al fine di aumentare il livello di sicurezza riguardo ad un possibile utilizzo improprio da parte di terzi delle proprie credenziali. I casi di applicazione obbligatoria del presente comma sono definiti con nota della Direzione.

3. L'utente è tenuto a scollegarsi dal sistema (log-out) ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro (PC) che utilizza, o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima. È vietato lasciare un PC incustodito connesso alla rete aziendale e/o ad Internet. L'eventuale utilizzo del PC da parte di soggetti non autorizzati non può essere dimostrato qualora l'accesso alla rete e/o Internet sia effettuato con le credenziali personali di un utente.

4. È ammessa solo la "navigazione" in siti della rete e/o di Internet considerati necessari all'espletamento della prestazione lavorativa: l'accesso ai siti Internet e/o alle risorse di rete è consentito secondo le policy di sicurezza aziendale che, opportunamente implementate e aggiornate, devono consentire la consultazione dei siti internet istituzionali (ad es. i siti: del Ministero della Sanità, delle Università, degli Enti locali). L'accesso ad Internet e lo sfruttamento delle sue numerose funzionalità (protocolli TCP/IP e programmi), è consentito esclusivamente per attività e finalità attinenti al proprio lavoro.

5. È vietato compiere azioni che siano in grado di arrecare danno all'ATS: in particolare è vietato il download, l'upload, il file sharing di software, file multimediali (video e musicali), lo scambio, la detenzione, la diffusione di file coperti da diritto d'autore o in violazione di licenze d'uso e/o brevetti; in generale, è vietato l'uso dei servizi di rete con finalità ludiche e/o, comunque, estranee all'attività lavorativa.

6. È vietato il download e l'upload di qualunque tipo di software gratuito (tipo freeware e shareware) da siti Internet, se non espressamente autorizzato dal Direttore Generale. È fatto altresì divieto all'utente di installare nei sistemi aziendali e nei PC assegnati dall'ATS prodotti software in violazione di licenze o diritto d'autore. E' vietato altresì l'utilizzo di servizi online per la gestione di dati aziendali riservati e/o soggetti a tutela della privacy (es. progettazione grafica, storage come google drive, conversione di documenti in formato pdf ad altro formato, etc..) in quanto le risorse online non hanno i requisiti di sicurezza sufficienti per poter trattare tali dati.

7. L'ATS ha facoltà di bloccare o limitare l'accesso a siti Internet ritenuti "pericolosi" attraverso l'utilizzo di idonei filtri (firewall); l'ATS adotterà ogni misura tecnica e tecnologica finalizzata a ridurre l'uso improprio della "navigazione" in Internet quando contrario al presente Regolamento e/o alla normativa vigente.

8. Di norma è vietata l'effettuazione di ogni genere di operazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo i casi in cui tali operazioni sia effettuate dalle UOC aziendali che dispongono pagamenti per conto dell'ATS quali ad esempio l'UOC Programmazione, Bilancio, Monitoraggio e Rendicontazione, l'UOC Risorse Umane e Organizzazione e i casi espressamente autorizzati dalla Direzione Generale,

9. È vietato - nell'orario di lavoro - l'utilizzo di abbonamenti privati effettuare la connessione a Internet tranne in casi del tutto eccezionali e previa autorizzazione del Direttore Generale. È comunque vietata ogni connessione ad internet da postazioni di ATS o che sfrutti la rete ATS mediante connessioni diverse da quelle espressamente autorizzate dal Direttore Generale o dal Direttore della UOC Sistemi Informativi Aziendali (es. abbonamenti privati di accesso ad internet.

10. È vietato il collegamento alla rete ATS di dispositivi HW come apparati di rete, dispositivi WiFi, sistemi di videosorveglianza o altri dispositivi IoT (Internet of Things), mentre per quanto riguarda PC e/o stampanti personali se non preventivamente autorizzati per iscritto dal Direttore della UOC Sistemi Informativi.

11. È vietato l'uso di PC aziendali o dell'infrastruttura telematica ATS per:

- effettuare l'accesso e/o la partecipazione a *forum* non professionali, a *chat line* (esclusi gli strumenti autorizzati), a bacheche elettroniche ovvero per effettuare accesso, utilizzo e registrazioni in *guest books* che prevedano l'utilizzo di identificativi personali oppure di pseudonimi (o nicknames);
- utilizzare l'indirizzo di posta elettronica aziendale per registrarsi su siti di carattere pubblico (es. facebook, pinterest, twitter, flickr, etc.) fatta eccezione per casi particolari contingenti all'ambito lavorativo;

se non nei casi in cui vi sia una espressa autorizzazione da parte della Direzione o delegati dalla stessa.

12. L'assegnazione agli utenti, ai dipendenti, ai collaboratori dell'ATS di Personal Computer (PC) o altri prodotti informatici non ne comporta l'uso a titolo privato, in quanto trattasi di strumenti di esclusiva proprietà di ATS e, quindi, i files memorizzati non sono né tutelati né garantiti dall'ATS per qualsiasi causa incidente sugli stessi. Tali dispositivi non possono essere utilizzati per uso personale né contenere documenti di carattere privato/personale.

ART. 5 UTILIZZO DEL PERSONAL COMPUTER

1. Il Personal Computer affidato al dipendente è uno strumento di lavoro; ognuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione; ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

2. Non è consentita l'attivazione della password d'accensione (firmware/bios), senza preventiva autorizzazione da parte della UOC Sistemi Informativi Aziendali.

3. Non è consentito all'utente modificare le caratteristiche hardware del proprio PC.

4. Non è consentita l'installazione di programmi diversi da quelli autorizzati dalla UOC Sistemi Informativi Aziendali.

5. Il Personal Computer di norma deve essere spento ogni sera prima di lasciare gli uffici fatta eccezione per i casi in cui venga chiesto di lasciarli accessi per attività di manutenzione straordinaria, in caso di assenze prolungate dall'ufficio, in caso di utilizzo remoto con accesso con VPN e in caso di attività in smart working .

6. Le informazioni archiviate in formato elettronico devono essere esclusivamente quelle previste e necessarie all'attività lavorativa.

7. Costituisce buona regola la pulizia periodica degli archivi (cartelle di file e posta elettronica), con cancellazione dei file obsoleti, inutili o duplicati da effettuarsi non meno di n 2 volte l'anno.

8. I dati lavorativi non devono essere conservati sui PC in dotazione agli utenti bensì nelle apposite aree di rete o in cloud (Sharepoint, Onedrive) messe a disposizione da ATS soggette a backup ed il cui accesso è controllato. I PC assegnati al personale non sono soggetti a backup.

9. I dati idonei a rivelare lo stato di salute e la vita sessuale dei pazienti devono essere salvati solo all'interno dei software in dotazione, specifici per il loro trattamento. Tali dati non devono essere conservati sui PC in dotazione degli utenti. Tale divieto vale anche in modo particolare per i dati di natura genetica dei pazienti.

10. È vietato l'uso di supporti di archiviazione removibili per la memorizzazione dei dati sensibili; ogni utilizzo di questi supporti da parte dell'utente oltre che essere considerato una violazione di tale divieto, è sotto la responsabilità dell'utente.

11. Gli operatori del Sistema Informativo possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza sui PC degli incaricati, sulle unità di rete e sugli spazi di archiviazione online (Onedrive, Sharepoint). L'utente ed il suo responsabile saranno informati qualora l'evento si dovesse verificare.

12. In caso di necessità urgenti di sicurezza, gli Amministratori di Sistema possono accedere ai dati contenuti nel PC dell'utente. L'accesso avverrà tramite le credenziali privilegiate dell'amministratore. L'utente è informato in caso di tale intervento.

ART. 6 UTILIZZO DI PC PORTATILI

1. L'utente è responsabile del PC portatile assegnatogli dall'ATS e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

2. Ai PC portatili si applicano le stesse regole di utilizzo previste per i PC fissi connessi in rete. L'utente di PC portatili deve prestare particolare attenzione alla rimozione di file, programmi e documenti che non possono, a causa dei dati e delle informazioni contenute, essere salvati o archiviati ovvero che contengono informazioni riservate o protette dalla vigente legislazione sulla privacy (con particolare riferimento al D. Lgs. n. 196/2003 e alle norme regolamentari emanate dall'ATS).

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

4. I PC portatili utilizzati all'esterno dei luoghi di lavoro (come in occasione di convegni, visite in aziende, workshop di lavoro, attività ispettive o di ricerca, attività in smart working), devono, in caso di allontanamento, essere custoditi in luogo protetto.

5. Nel caso di accesso a Internet tramite la rete ATS l'utente deve osservare le seguenti prescrizioni:

- utilizzare l'accesso in forma esclusivamente personale;
- utilizzare le credenziali (es. la password) in modo rigoroso;
- disconnettersi dalla rete aziendale al termine della sessione di lavoro;
- collegarsi periodicamente alla rete interna per consentire gli aggiornamenti del sistema operativo, delle policy di gestione e delle definizioni antivirus.

ART. 7 UTILIZZO DI TELEFONI E TABLET PER L'ACCESSO A RISORSE CLOUD DI ATS

Sui telefoni aziendali è consentito installare/utilizzare esclusivamente applicazioni strettamente correlate con l'attività lavorativa (Teams, Sharepoint, Onedrive, Outlook,

Office, Multi Factor Authenticator).

Per risorse Cloud di ATS si intendono i servizi di Office 365 (posta elettronica, SharepointOnline, Ondrive, Teams).

L'utilizzo di tali risorse, attraverso dispositivi mobili (telefoni e tablet) personali e/o aziendali, è consentito nel rispetto dei seguenti "requisiti":

1) Provvedere all'installazione degli aggiornamenti del sistema operativo e delle applicazioni quando richiesto dal sistema.
2) Non modificare l'immagine del sistema operativo o le impostazioni di sicurezza di fabbrica come ad esempio la rimozione delle protezioni del dispositivo, rooting o upload di firmware non forniti dal vendor.
3) Utilizzare solo connessioni Wi-fi che garantiscano un livello minimo di sicurezza. Evitare ad esempio l'accesso ad access point wi-fi gratuiti.
4) Configurare la cifratura del dispositivo per rendere impossibile l'accesso ai dati in caso di smarrimento.
5) Le risorse Cloud di cui ATS devono essere accedute solo attraverso app certificate dal vendor dei servizi tramite cui vengono rese disponibili le risorse stesse.

ART. 8 CORRETTO UTILIZZO DELLA POSTA ELETTRONICA

1. L'ATS si riserva la facoltà di attivare indirizzi di posta elettronica per le UU.OO., condivisi dagli operatori (utenti e/o gruppi di utenti) assegnati a ciascuna di esse (es.: nomestruttura@ats-milano.it). Al singolo lavoratore dipendente è assegnato un indirizzo e-mail personale del tipo: ncognome@ats-milano.it.

2. In ogni caso, la "personalizzazione" dell'indirizzo di posta elettronica non comporta l'attribuzione di un carattere "privato", in quanto trattasi di strumenti di esclusiva proprietà di ATS, messi a disposizione del dipendente al solo fine dello svolgimento delle proprie mansioni lavorative. Il contenuto della casella di posta elettronica è accessibile, secondo le procedure previste dal presente regolamento **(art. 8 – comma 6 - e art. 10)** e dalle norme regolamentari emanate dalla ATS nonché in conformità alle vigenti leggi.

3. La diffusione massiva (gruppi di destinatari) di messaggi di posta elettronica deve essere effettuata esclusivamente per motivi inerenti il servizio, su autorizzazione del Dirigente

responsabile di Dipartimento o di Struttura Complessa (UOC). L'uso di messaggi con destinazione "LD Tutti" è vietato salvo autorizzazione preventiva della Direzione Generale.

4. ATS mette a disposizione di ciascuna Organizzazione Sindacale e della RSU una bacheca sindacale in cui possono essere pubblicati i messaggi per i dipendenti che vogliano prenderne visione. A tal fine, ciascuna Sigla Sindacale e la RSU individuano il nominativo di un dipendente e di un supplente autorizzati a trasmettere messaggi di posta elettronica con destinazione massiva, riportanti il rinvio alla bacheca del Sindacato.

5. Non è consentito diffondere catene telematiche del tipo "catena di S. Antonio" o di tipologia simile anche se il contenuto sembra meritevole di attenzione; in particolare gli appelli di solidarietà ed i messaggi che informano dell'esistenza di nuovi virus. In generale, è vietato l'invio di messaggi pubblicitari di prodotti o servizi di qualsiasi tipo.

6. In caso di assenza prolungata e per improrogabili necessità, dovrà essere attivata la funzione autoreply o l'inoltro automatico su altre caselle aziendali a cura del dipendente. In caso di assenza improvvisa del dipendente, la funzione di autoreply e l'inoltro automatico su altre caselle aziendali potranno essere attivate – a cura della UOC Sistemi Informativi Aziendali – su richiesta motivata del Dirigente responsabile della UO (UOC, UOSD, UOS). In casi di stretta necessità, qualora si debba conoscere il contenuto dei messaggi ricevuti in posta elettronica istituzionale del dipendente assente o in caso di impedimento, ATS potrà accedere alla casella di posta su richiesta motivata del Dirigente responsabile della UO(UOC, UOSD, UOS), previo parere favorevole del Direttore di Dipartimento o del Direttore Strategico di riferimento – in forma scritta - con obbligo di informazione per il lavoratore interessato mediante nota – inoltrata con PEC o con raccomandata A/R - in cui sono illustrate le motivazioni di tale accesso.

7. Nei messaggi inviati tramite posta elettronica diretti verso l'esterno dell'ATS verrà accluso in maniera automatica dal sistema di posta il testo che riporta la politica di ATS in materia di privacy e in particolare la non divulgabilità delle informazioni.

In sede di prima applicazione il testo è il seguente:

"Ai sensi del D.lgs. n. 196 del 30.06.03 (Codice Privacy), le informazioni contenute nella

presente comunicazione sono riservate e ad uso esclusivo del destinatario. La diffusione, distribuzione e/o fotocopiatura del presente documento e di eventuali allegati da parte di qualsiasi soggetto diverso dai destinatari è proibita; tale divieto di diffusione è sanzionato sia dall'art. 616 c.p. (violazione, sottrazione e soppressione di corrispondenza) che dal D.Lgs. 196/03. Qualora il messaggio fosse pervenuto per errore, La preghiamo di eliminarlo senza copiarlo ovvero inoltrarlo a terzi, dandocene gentilmente immediata comunicazione".

Il testo potrà essere modificato e revisionato mediante nota scritta del Direttore Generale.

8. È consentito l'utilizzo dei PC e della infrastruttura di rete dell'ATS per l'accesso a sistemi di Internet nonché di servizi di webmail personali per assolvere incombenze amministrative e burocratiche senza allontanarsi dal luogo di lavoro (ad esempio: per effettuare adempimenti on-line nei confronti di Pubbliche Amministrazioni e di concessionari di servizi pubblici, ovvero per tenere rapporti con istituti bancari), nei casi eccezionali in cui la comunicazione mediante internet risulta più conveniente – per tempistica o necessità - rispetto all'uscita dal servizio.

9. Si deve evitare, secondo le regole di buona diligenza, l'apertura e lettura di messaggi di posta elettronica in arrivo provenienti da mittenti di cui non si conosce con certezza l'identità o che contengano allegati di tipo *.exe, *.com, *.vbs, *.htm, *.scr, *.bat, *.js e *.pif, in qualunque altra situazione di incertezza contattare la UOC Sistemi Informativi Aziendali, mediante i servizi di help desk.

ART. 9 SISTEMI DI ARCHIVIAZIONE ONLINE E COMUNICAZIONE

1. È vietato effettuare la condivisione di informazioni interne, riservate o sensibili utilizzando la condivisione anonima (in cui non è specificato uno specifico utente o gruppo di destinatari) tramite strumenti quali Sharepoint e Onedrive.

2. Le condivisioni devono essere mantenute attive per un arco temporale minimo indispensabile allo scopo per il quale sono state create.

3. È necessario verificare periodicamente, almeno una volta al mese, le condivisioni attivate ed eliminare quelle non più che necessarie.

4. È vietato l'utilizzo di strumenti di condivisione esterni ai sistemi cloud di ATS (Onedrive, Sharepoint) come ad esempio Wetransfer, Google drive, per la condivisione di materiale con altri enti/istituzioni. Tali sistemi infatti potrebbero non essere compatibili con la normativa europea in materia di privacy e/o non rispettare le policy di sicurezza di ATS.

ART. 10 CONTROLLI DISPOSTI DALL'ATS

1. Nel rispetto dei principi **di pertinenza e di non eccedenza** ed evitando una interferenza ingiustificata **sui diritti e sulle libertà fondamentali dei lavoratori**, così come la possibilità di controlli, costanti o indiscriminati, l'ATS può di effettuare controlli sull'uso degli strumenti informatici e telematici aziendali.

2. Il controllo di cui al comma precedente scaturirà:

- dalla necessità di dovere effettuare verifiche sulla funzionalità e sicurezza del sistema;
- su segnalazione e/o esposti dell'autorità giudiziaria, di cittadini purché non anonimi e delle autorità di vigilanza;
- dal rilevamento di anomalie nell'utilizzo della rete aziendale e/o dell'accesso e uso di Internet.

3. I controlli saranno svolti dal personale in servizio presso la UOC Servizi Informativi Aziendali, con la supervisione del Direttore della UOC Sistemi Informativi Aziendali. È ammesso il ricorso a professionalità esterne, ferma restando la supervisione del Direttore della UOC Sistemi Informativi Aziendali. Tale supervisione non sarà necessaria nel caso di controllo su segnalazione e/o ordine dell'autorità giudiziaria e/o di indagine nonché in caso di controllo fondato su esposti - non anonimi- riguardante -in tutto o in parte- l'attività del citato Direttore e/o degli operatori della UOC Sistemi Informativi Aziendali.

4. Il controllo sarà svolto, **in via preliminare**, su **dati aggregati** relativi, a seconda dei casi, all'ATS, ai Dipartimenti, alle Direzioni, alle Strutture Complesse (UOC), alle Strutture Semplici (UOS), alle Strutture Semplici Dipartimentali (UOSD), agli Uffici con almeno cinque dipendenti.

5.Nell'ipotesi in cui da tale forma di **controllo anonimo** su dati aggregati dovesse scaturire un utilizzo anomalo degli strumenti aziendali, l'ATS emetterà un invito – rivolto ai **Dirigenti, e**

per il loro tramite, ai dipendenti afferenti alla realtà lavorativa interessata – di attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

6. Qualora l'anomalia dovesse ripetersi e riguardare lo stesso ambito lavorativo, l'ATS, dopo l'avviso di cui al comma precedente, procederà ad effettuare **controlli su base individuale**.

7. Non si applicano le condizioni di cui al comma 4 e 5 nel caso di segnalazione/esposti/ordini dell'autorità giudiziaria.

ART. 11 CONSERVAZIONE DEI DATI

1. In applicazione dei principi di diritto di accesso, legittimità, proporzionalità, sicurezza ed accuratezza e conservazione dei dati, le informazioni relative all'accesso ad Internet ed al traffico telematico la cui conservazione non sia necessaria, saranno cancellate entro sei mesi dalla loro produzione.

2. È consentito il prolungamento dei tempi di conservazione in casi specifici, ad es.: per esigenze tecniche o di sicurezza; per l'indispensabilità dei dati rispetto all'esercizio od alla difesa di un diritto in sede giudiziaria o, infine, all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

ART. 12 SMART WORKING

1. Il presente regolamento si applica anche nel caso di Smart Working: istituto disciplinato dalla legge 22 maggio 2017 n.81 (Misure per la tutela del lavoro autonomo non imprenditoriale e misure volte a favorire l'articolazione flessibile nei tempi e nei luoghi del lavoro subordinato), al Capo II, ed in particolare dall'art.18 all'art.23. Lo Smart Working è una: «tipologia di lavoro senza precisi vincoli di orario o di luogo di lavoro, con il possibile utilizzo di strumenti tecnologici per lo svolgimento dell'attività lavorativa».

2. Nel caso di utilizzo di strumenti messi a disposizione da ATS, il dipendente in Smart Working è personalmente responsabile della sicurezza, custodia e conservazione in buono stato, salvo l'ordinaria usura derivante dall'utilizzo, delle dotazioni informatiche eventualmente fornitegli dall'amministrazione.

3. Le dotazioni informatiche dell'ATS devono essere utilizzate esclusivamente per ragioni di servizio, ma non devono subire alterazioni della configurazione di sistema, ivi inclusa la parte relativa alla sicurezza, e su queste non devono essere effettuate installazioni di software non autorizzate.

4. Il lavoratore è tenuto agli obblighi di riservatezza, ai sensi del DPR 16 aprile 2013 n.62 «Regolamento recante codice di comportamento dei dipendenti pubblici» e agli altri obblighi previsti nel Codice di comportamento dei dipendenti di ATS.

ART. 13 SANZIONI DISCIPLINARI

1. Tutte le violazioni al presente regolamento potranno essere oggetto di procedimento disciplinare, fatte salve le ulteriori responsabilità civili, penali e contabili previste dalla normativa vigente.

2. Si rimanda ai CCNL, CCIA, al regolamento ATS sui procedimenti disciplinari, al codice di comportamento di ATS nonché al D. Lgs 165/2001.

ART. 14 DISPOSIZIONI FINALI

1. È fatto obbligo, a chiunque spetti, di osservare e far osservare il presente regolamento. Per quanto non espressamente previsto nel presente regolamento, si rinvia ai regolamenti aziendali in materia di accesso agli atti, di procedimento amministrativo e di privacy nonché alla normativa nazionale e regionale vigente.

2. Il presente regolamento si compone di n. 14 (quattordici) articoli, per n. 18 (diciotto) pagine complessive che ricomprendono – a partire dalla pagina 16 (sedici) – "Definizioni e acronimi".

3. Il presente regolamento entra in vigore al quindicesimo giorno di pubblicazione del provvedimento deliberativo di adozione.

DEFINIZIONI E ACRONIMI

Chat line – *Il termine chat (in inglese, letteralmente, "chiacchierata"), viene usato per riferirsi a un'ampia gamma di servizi sia telefonici che via Internet; ovvero, complessivamente, quelli che i paesi di lingua inglese distinguono di solito con l'espressione "online chat", "chat in linea". Questi servizi, anche piuttosto diversi fra loro, hanno tutti in comune due elementi fondamentali: il fatto che il dialogo avvenga in tempo reale, e il fatto che il servizio possa mettere facilmente in contatto perfetti sconosciuti, generalmente in forma essenzialmente anonima. Il "luogo" (lo spazio virtuale) in cui la chat si svolge è chiamato solitamente chatroom (letteralmente "stanza delle chiacchierate"), detto anche channel (in italiano canale), spesso abbreviato chan.*

Credenziali -credenziali informatiche – *Il sistema di autenticazione per l'accesso ai servizi consiste in un codice per l'identificazione dell'incaricato ("username"), associato ad una parola chiave riservata ("password") conosciuta esclusivamente dall'utente e i due elementi costituiscono una cosiddetta credenziale di autenticazione ("account o "user-id") ai sensi dell'allegato B punto 2 DLGS 196/03 e succ. mod. Lo username viene assegnato e variato esclusivamente dall'amministratore di sistema – ove delegato dal Direttore della s.c. Sistema Informativo Aziendale. La password viene gestita, dopo la sua prima assegnazione, esclusivamente dall'utente, con l'eccezione dei casi in cui ricorrano necessità di carattere tecnico-organizzative. Analogamente si procede per le credenziali di autenticazione riguardanti la posta elettronica se non esiste un sistema unificato delle credenziali di autenticazione.*

Download o upload – *In generale con questo termine si intende il trasferimento di dati da un computer locale a uno remoto utilizzando un apparato di comunicazione, ad es. il modem, o tra computer della stessa rete. Per download si intende anche la visualizzazione sul proprio computer di una pagina Internet.*

File sharing – *è la condivisione di file all'interno di una rete comune. Può avvenire attraverso una rete con struttura client-server (cliente-servente) oppure peer-to-peer (pari a pari). Le più famose reti di peer-to-peer sono: Gnutella, OpenNap, Bittorrent, eDonkey, Kademlia. Non vanno confuse con reti che costituiscono un filesystem distribuito, come Freenet. Queste reti possono permettere di individuare più copie dello stesso file nella rete per mezzo di hash crittografici, di riprendere lo scaricamento del*

file, di eseguire lo scaricamento da più fonti contemporaneamente, di ricercare un file in particolare per mezzo di un URI Universal Resource Identifier. programmi di file-sharing, sono utilizzati direttamente o indirettamente per trasferire file da un computer ad un altro su Internet, o su reti aziendali Intranet. Questa condivisione ha dato origine al modello peer-to-peer.

Forum – *(plurale in latino fora) - è utilizzata in italiano per indicare l'insieme delle sezioni di discussione in una piattaforma informatica, una singola sezione, oppure il software utilizzato per fornire questa struttura (detto anche "board"). Una comunità virtuale si sviluppa spesso intorno ai forum (es. Facebook, che può essere definito "strumento integrato di servizi, social network forum based), nel quale scrivono utenti abituali con interessi comuni. I forum vengono utilizzati anche come strumento di assistenza online e all'interno di aziende per mettere in comunicazione i dipendenti e permettere loro di reperire informazioni. Ci si riferisce comunemente ai forum anche con termini e locuzioni in lingua inglese come: board, message board, bulletin board oppure gruppi di discussione, bacheche e altri. Molti forum richiedono la registrazione dell'utente prima di poter inviare messaggi e in alcuni casi anche per poterli leggere. Diversamente dalla chat, che è uno strumento di comunicazione sincrono, ovvero nel quale la comunicazione avviene nello stesso momento, il forum è asincrono, in quanto la scrittura e la risposta può avvenire in momenti diversi.*

Password – *vedi la voce Credenziali*

Posta elettronica o e-mail – *dall'inglese «electronic mail» - è un servizio Internet grazie al quale ogni utente può inviare e ricevere dei messaggi mediante l'utilizzo di protocolli costituenti l'infrastruttura tecnologica di Internet (es. POP3, SMTP, IMAP). È l'applicazione Internet più conosciuta e più utilizzata attualmente. È la controparte digitale ed elettronica della posta ordinaria e cartacea.*

Rete telematica – *è un sistema di comunicazione che permette l'interconnessione di strutture telefoniche ed informatiche che servono diverse classi di utenti distribuiti su un'area più o meno ampia.*
Oggi si definisce con "rete telematica" l'insieme delle reti di calcolatori e dei servizi di telefonia. La rete telematica è Basata spesso sugli stessi protocolli usati per Internet: è possibile collegare ogni rete telematica ad

Per funzionare, gli elementi all'interno di una rete telematica devono seguire delle regole comuni: col termine protocollo si definisce l'insieme di regole e di messaggi che governano la comunicazione tra due entità.

Username – *vedi la voce Credenziali*

***.exe, *.com, *.vbs, *.htm, *.scr, *.bat, *.js e *.pif –** *Si tratta di estensione di file che mandano in esecuzione file eseguibili che, a loro volta, possono infettare il computer con un virus.*