Azienda Territoriale per l'Edilizia Residenziale
Pubblica della Provincia di Viterbo

Via Igino Garbini,78/A – 01100 Viterbo Tel. 0761/2931 Fax.761/227303 C.F. 80000910564 P.IVA 00061420568

REGOLAMENTO AZIENDALE
PER LA GESTIONE E L'UTILIZZO DELLE RISORSE STRUMENTALI INFORMATICHE E TELEMATICHE

Approvato con deliberazione del Consiglio di Amministrazione n.11 del 09.06.2022

INDICE

Premessa

Il sistema informativo dell'ATER di Viterbo è costituito dall'insieme del patrimonio informativo digitale e dalle risorse tecnologiche ed organizzative che acquisiscono, elaborano, rendono disponibili ed utilizzano tale patrimonio informativo. Le risorse tecnologiche sono l'insieme degli strumenti hardware e software che permettono di accedere al patrimonio informatico digitale dell'Azienda, nonché alle risorse informative esterne collegate alla rete dell'Azienda tramite reti pubbliche e private. Il presente Regolamento intende fornire ai dipendenti e collaboratori, denominati anche incaricati o utenti, le indicazioni per una corretta e adeguata gestione delle informazioni, in particolare attraverso l'uso di sistemi, applicazioni e strumenti informatici dell'Ente. Ogni dipendente e collaboratore è tenuto a rispettare il Regolamento, che è reso disponibile tramite le modalità specificate dall'art.16. Si specifica che tutti gli strumenti utilizzati dal lavoratore, intendendo con ciò PC Desk, notebook, risorse, e-mail ed altri strumenti con relativi software e applicativi (di seguito più semplicemente "Strumenti"), sono messi a disposizione dall'Ente per rendere la prestazione lavorativa. Gli Strumenti, nonché le relative reti a cui è possibile accedere tramite gli stessi, sono domicilio informatico dell'Ente. I dati personali e le altre informazioni dei dipendenti e collaboratori registrati negli Strumenti o che si possono eventualmente raccogliere tramite il loro uso, sono utilizzati per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio. Per tutela del patrimonio si intende altresì la sicurezza informatica e la tutela del sistema informatico. Tali informazioni sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, visto che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo 679/2016 "*General Data Protection Regulation*". Viene, infine, precisato che non sono installati o configurati sui sistemi informatici in uso ai dipendenti/collaboratori apparati hardware o strumenti software aventi come scopo il controllo a distanza dell'attività dei lavoratori.

Art. 1 - Oggetto e Finalità

Il presente Regolamento è redatto:

- alla luce della Legge 20/05/1970, 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*";
- in attuazione del Regolamento Europeo 679/2016 "*General Data Protection Regulation*" (d'ora in avanti Reg. 679/2016 o GDPR);
- ai sensi delle "*Linee guida del Garante per posta elettronica e internet*" in Gazzetta Ufficiale n. 58 del 10 marzo 2007;
- alla luce dell'articolo 23 del D. Lgs. n.151/2015 (c.d. *Jobs Act*) che modifica e rimodula la fattispecie integrante il divieto dei controlli a distanza, nella consapevolezza di dover tener conto, nell'attuale contesto produttivo, oltre agli impianti audiovisivi, anche degli altri strumenti "*dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori"* e di quelli *"utilizzati dal lavoratore per rendere la prestazione lavorativa",* e del conseguente Accordo Quadro di *"Utilizzo Impianti di video sorveglianza",* approvato con le OO.SS. in data 21/05/2021.

Il presente Regolamento disciplina:

- le modalità di accesso ed utilizzo degli strumenti informatici, della rete informatica e dei servizi che tramite la stessa rete è possibile ricevere ed offrire all'interno e all'esterno dell'Azienda, nell'ambito dello svolgimento delle proprie mansione ed attività di ufficio dei dipendenti e collaboratori;
- l'individuazione del complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione per il trattamento dei dati personali, al fine di garantire l'aderenza e la rispondenza alle vigenti normative in materia, nonché gli adeguati livelli di sicurezza ed integrità del patrimonio informativo dell'Azienda.

LA FINALITÀ DEL REGOLAMENTO È DI PROMUOVERE IN TUTTO IL PERSONALE UNA CORRETTA "CULTURA INFORMATICA" AFFINCHÉ L'UTILIZZO DEGLI STRUMENTI INFORMATICI E TELEMATICI FORNITI DALL'ENTE, QUALI LA POSTA ELETTRONICA, INTERNET E I PERSONAL COMPUTER CON I RELATIVI SOFTWARE, SIA CONFORME ALLE FINALITÀ E NEL PIENO RISPETTO DELLA LEGGE. SI VUOLE FORNIRE A TUTTO IL PERSONALE LE INDICAZIONI NECESSARIE CON L'OBIETTIVO PRINCIPALE DI EVITARE IL VERIFICARSI DI QUALSIASI ABUSO O USO NON CONFORME, MUOVENDO DALLA CONVINZIONE CHE LA PREVENZIONE DEI PROBLEMI SIA PREFERIBILE RISPETTO ALLA LORO SUCCESSIVA CORREZIONE

Art. 2 -Principi generali: figure coinvolte e riservatezza nelle comunicazioni

1.Nell'ambito della gestione delle risorse e dei servizi informatici aziendali, risultano essere coinvolte diverse figure: il funzionario **Responsabile dei Sistemi Informatici** che opera in stretta collaborazione con l'**Amministratore di Sistema** in carica, in modo da contribuire allo svolgimento dei numerosi e complessi compiti che questi soggetti, ognuno per le proprie competenze e rispettive responsabilità, sono chiamati ad assicurare per il funzionamento dell'infrastruttura informatica. Questi profili sono coordinati dal **Responsabile per la Transizione al Digitale** (RTD) - previsto dal Codice dell'Amministrazione Digitale, (D. Lgs.82/2005) - che deve garantire operativamente la trasformazione digitale della Pubblica Amministrazione, attraverso lo sviluppo dei servizi pubblici digitali e l'adozione di modelli di relazione trasparenti e aperti con i cittadini, anche attraverso ulteriori figure nominate all'interno e all'esterno dell'Amministrazione quali: il **Responsabile della Gestione Documentale** (DPR 28 dicembre 2000, n. 445 art. 61 co. 2; DPCM 3 dicembre 2013, art. 4), figura chiave per la dematerializzazione dei processi, cui spetta, tra le altre cose, predisporre lo schema del manuale di gestione documentale, che deve essere coerente con il piano di digitalizzazione dell'ente. Lo stesso CAD richiama espressamente la necessità che il responsabile del sistema di gestione dei documenti informatici operi d'intesa con l'RTD (art. 44, co. 1-bis); Il **Responsabile per la Protezione dei Dati Personali** (art. 37 del Reg. 679/2016): figura chiamata ad assolvere funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione della normativa in materia di protezione dei dati personali. Il coordinamento con il RTD è fondamentale per lo sviluppo di sistemi informativi e servizi online conformi ai principi data *protection by default* e *by design;* Il **Responsabile della Prevenzione della Corruzione e della Trasparenza** (legge 190/2012, art. 1, co. 7 come modificato dal d.lgs. 97/2016): la collaborazione tra le due figure è in questo caso essenziale per garantire che l'applicazione delle tecnologie ai processi di riorganizzazione dell'ente rispondano a adeguate caratteristiche di trasparenza e ai principi dell'amministrazione aperta.

2. I principi che sono a fondamento del presente Regolamento sono gli stessi espressi nel GDPR, e, precisamente:

- **il principio di necessità,** secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 5 e 6 del Reg.679/2016);
- **il principio di correttezza,** secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori. Le tecnologie dell'informazione (in modo più marcato rispetto ad apparecchiature tradizionali) permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa. Ciò, all'insaputa o senza la piena consapevolezza dei lavoratori, considerate anche le potenziali applicazioni di regola non adeguatamente conosciute dagli interessati;
- **i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime** (art.5 commi 1 e 2 del Reg. 679/2016), osservando il principio di pertinenza e non eccedenza. Il datore di lavoro deve trattare i dati *"nella misura meno invasiva possibile";* le attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere *"mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza"*.

Art. 3 - Tutela del lavoratore

1. Alla luce dell'art. 4, comma 1, L. n. 300/1970, la regolamentazione della materia di cui all'art.1 del presente Regolamento, non è finalizzata all'esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro, ma solo a permettere a quest'ultimo di utilizzare sistemi informativi per fare fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali.

2. È garantito al singolo lavoratore il controllo sui propri dati personali secondo quanto previsto dagli articoli 15-16-17-18-20-21-77 del Reg. 679/2016.

Art.4 - Campo di applicazione

Il presente regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o di livello, nonché a tutti i collaboratori dell'Ente a prescindere dal rapporto contrattuale intrattenuto con lo stesso. Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente e collaboratore in possesso di specifiche credenziali di autenticazione. Tali figure, a seconda delle funzioni svolte, vengono nominate dal Titolare quali "responsabili del trattamento" o "incaricati del trattamento" ai sensi del Regolamento 679/2016.

Art. 5 - Gestione, assegnazione e revoca delle credenziali di accesso

1. Le credenziali di autenticazione per l'accesso alle risorse informatiche vengono assegnate dall'Amministratore di Sistema, previa formale richiesta al Responsabile dei Sistemi Informatici da parte del Responsabile dell'ufficio/area nell'ambito del quale è inserito ed andrà ad operare il nuovo utente. Nel caso di collaboratori esterni la richiesta dovrà essere inoltrata direttamente dalla Direzione Generale o dal Responsabile dell'ufficio/area con il quale il collaboratore si coordina nell'espletamento del proprio incarico. La richiesta di attivazione delle credenziali dovrà essere completa di generalità dell'utente ed elenco dei sistemi informativi per i quali deve essere abilitato l'accesso. Ogni eventuale successiva variazione delle abilitazioni di accesso ai sistemi informativi dovrà seguire lo stesso iter procedurale.

2. Le credenziali di autenticazione consistono in un codice per l'identificazione del dipendente/collaboratore (altresì nominati username, nome utente o user id), assegnato dall'Amministratore di Sistema, ed una relativa password temporanea. La password è personale e riservata e dovrà essere conservata e custodita dall'incaricato con la massima diligenza senza divulgarla così come previsto dal Manuale della Data Privacy dell'Azienda.

3. La password deve essere di adeguata robustezza: deve essere composta da almeno 8 caratteri, formata da lettere maiuscole e minuscole e/o numeri/caratteri speciali. Non deve contenere riferimenti agevolmente riconducibili al dipendente/collaboratore (username, nomi o date relative alla persona o ad un familiare).

4. È necessario che il dipendente/collaboratore al primo accesso, proceda alla modifica della password temporanea trasmessa dall'Amministratore di Sistema, successivamente lo stesso utente dovrà modificarla almeno ogni 60 giorni così come il sistema richiederà periodicamente in automatico.

5. Nel caso di necessità di rilascio di una nuova password, l'utente dovrà comunicare al proprio Responsabile dell'Ufficio/area la necessità di aggiornamento delle credenziali giustificandone i motivi, la richiesta sarà trasmessa al Responsabile dei Sistemi Informatici e per conoscenza al DPO. Il Responsabile dei Sistemi Informatici provvederà tramite l'Amministratore di Sistema al rilascio delle nuove credenziali;

6. In caso di cessazione dell'utenza il Responsabile dell'Ufficio/area competente inoltrerà la richiesta specificando la data effettiva a partire dalla quale le credenziali dell'utente dovranno essere disabilitate, sarà cura del Responsabile dei Sistemi Informatici operare per rendere effettive le modifiche tramite l'Amministratore di Sistema.

Art. 6 - Utilizzo infrastruttura di rete e FileSystem

1. Per l'accesso alle risorse informatiche dell'Ente attraverso la rete locale, ciascun dipendente/collaboratore deve essere in possesso di credenziali di autenticazione secondo quanto stabilito nel precedente Art. 5 - Gestione, assegnazione e revoca delle credenziali di accesso. È assolutamente proibito accedere alla rete ed ai sistemi informativi utilizzando credenziali di altre persone.

2. L'accesso alla rete garantisce al dipendente/collaboratore la disponibilità di condivisioni di rete (cartelle su server) nelle quali vanno obbligatoriamente inseriti e salvati i files di lavoro, organizzati per area/uffici/gruppi o per diversi criteri o per obiettivi specifici di lavoro. Tutte le cartelle locali e di rete, siano esse condivise o personali, possono ospitare esclusivamente contenuti professionali. Pertanto è vietato il salvataggio sui server dell'Ente, ovvero sugli Strumenti, di documenti non inerenti le attività lavorative, quali a titolo esemplificativo documenti, fotografie, video, musica, pratiche personali, sms, mail personali, film e quant'altro. Ogni materiale personale rilevato dall'Amministratore di Sistema a seguito di interventi di sicurezza informatica ovvero di manutenzione/aggiornamento su server ed anche su Strumenti, verrà rimosso secondo le regole previste nel successivo art. 12 del presente Regolamento, ferma ogni ulteriore responsabilità civile, penale e disciplinare. Tutti gli spazi virtuali utilizzati condivisi sui server sono sottoposti a backup periodici.

3. Senza il consenso del Responsabile dei Sistemi Informativi, è vietato trasferire documenti elettronici dai sistemi informativi e Strumenti dell'Ente a device esterni (hard disk, chiavette, CD, DVD e altri supporti), o salvare documenti elettronici dell'Ente (ad esempio pervenuti via mail o salvati sul Server o sullo Strumento in dotazione) su repository esterne (quali ad esempio Dropbox, Google Drive, OneDrive, ecc.) ovvero inviandoli a terzi via posta elettronica o con altri sistemi.

4. Con regolare periodicità è necessario che ogni utilizzatore si assicuri sullo stato di aggiornamento del proprio sistema operativo, in modo da garantire il corretto funzionamento di ogni singola postazione garantendo l'applicazione delle *patch* e dei *fix* di sicurezza, così come rilasciate dal produttore del sistema operativo adottato o da specifiche segnalazioni provenienti dal Responsabile dei Sistemi Informatici e/o dall'Amministratore di Sistema e dal DPO, su ogni postazione di lavoro; ciascun dipendente/collaboratore provvederà, inoltre, alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

5. L'Ente mette a disposizione dei propri dipendenti la possibilità di accedere alle proprie risorse informatiche anche dall'esterno mediante: l'utilizzo di un pc notebook in dotazione personale con all'interno un software antivirus *Endpoint Protection* e di sicurezza *Device Encryption* per la protezione dei dati presenti da e verso il cloud; una rete VPN (Virtual Private Network), un canale privato e criptato verso la rete interna. L'accesso mediante VPN viene concesso ai dipendenti dell'Ente che necessitino di svolgere compiti lavorativi, pur non essendo presenti in sede *(ad esempio per lo smart working)*. Le richieste di abilitazione all'accesso mediante VPN dovranno seguire le prescrizioni dell'art. 5 - Gestione, assegnazione e revoca delle credenziali di accesso, per motivi di sicurezza la fase di autenticazione è implementata con un ulteriore sistema così detto "a più fattori" o *strong authentication* che punta così a limitare al massimo i possibili rischi derivanti da attacchi *hacker*.

6. All'interno delle sedi lavorative è resa disponibile anche una rete senza fili, c.d. "Wi-Fi". Tali reti consentono l'accesso alle risorse e ad internet per i dispositivi non connessi alla rete LAN mediante cavo. L'accesso mediante rete Wi-Fi viene concesso a consulenti, professionisti, tecnici e fornitori che nell'ambito di un rapporto contrattuale con l'Ente necessitino di accedere a determinate risorse informatiche. Viene concesso, altresì, a dipendenti e collaboratori dell'Ente che necessitino di svolgere compiti specifici che non possono essere svolti dalle postazioni fisse. La richiesta di attivazione dovrà essere presentata alla Direzione Generale per la necessaria autorizzazione ed in copia al Responsabile dei Sistemi Informatici che provvederà in merito tramite l'Amministratore di Sistema.

7. L'Amministratore di Sistema si riserva la facoltà di negare o interrompere l'accesso alla rete mediante dispositivi non adeguatamente protetti e/o aggiornati, che possano costituire una concreta minaccia per la sicurezza informatica.

I LOG RELATIVI ALL'USO DEL FILE SYSTEM E DELLA INTRANET, NONCHÉ I FILE SALVATI O TRATTATI SU SERVER O STRUMENTI, SONO REGISTRATI E POSSONO ESSERE OGGETTO DI CONTROLLO DA PARTE DEL TITOLARE DEL TRATTAMENTO, ATTRAVERSO L'AMMINISTRATORE DI SISTEMA, PER ESIGENZE ORGANIZZATIVE E PRODUTTIVE, PER LA SICUREZZA DEL LAVORO E PER LA TUTELA DEL PATRIMONIO. I CONTROLLI POSSONO AVVENIRE SECONDO LE DISPOSIZIONI PREVISTE AL SUCCESSIVO ART. 12 DEL PRESENTE REGOLAMENTO. LE INFORMAZIONI COSÌ RACCOLTE SONO ALTRESÌ UTILIZZABILI A TUTTI I FINI CONNESSI AL RAPPORTO DI LAVORO, COMPRESA LA VERIFICA DEL RISPETTO DEL PRESENTE REGOLAMENTO, CHE COSTITUISCE ADEGUATA INFORMAZIONE DELLE MODALITÀ D'USO DEGLI STRUMENTI E DI EFFETTUAZIONE DEI CONTROLLI AI SENSI DEL REGOLAMENTO EUROPEO 679/2016 "*GENERAL DATA PROTECTION REGULATION*".

Art. 7 - Utilizzo degli Strumenti elettronici (PC, notebook e altri strumenti con relativi software e applicativi)

1. Il dipendente/collaboratore è consapevole che gli Strumenti forniti sono di proprietà dell'Ente e devono essere utilizzati esclusivamente per rendere la prestazione lavorativa. Ognuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione. Ogni utilizzo non inerente l'attività lavorativa è vietato in quanto può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Ciascun dipendente /collaboratore si deve quindi attenere alle seguenti regole di utilizzo degli Strumenti.

2. L'accesso agli Strumenti è protetto da password; per l'accesso devono essere utilizzati Username e password assegnate dall'Amministratore di Sistema (cfr. - Gestione, assegnazione e revoca delle credenziali di accesso). A tal proposito si rammenta che essi sono strettamente personali ed il dipendente/collaboratore è tenuto a conservarli nella massima segretezza.

3. Il Personal Computer, notebook, tablet ed ogni altro dispositivo deve essere custodito con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento e segnalando tempestivamente al Responsabile dei Sistemi Informatici ogni eventuale malfunzionamento e/o danneggiamento. Non è consentita l'attivazione della password d'accensione (BIOS), senza preventiva autorizzazione da parte dell'Amministratore di Sistema.

4. Non è consentito al dipendente/collaboratore modificare le caratteristiche hardware e software impostate sugli Strumenti assegnati, salvo preventiva circostanziata richiesta al Responsabile dei Sistemi Informatici che provvederà in merito ad attivare l'Amministratore di Sistema.

5. L’utente è tenuto a scollegarsi dal sistema, o bloccare l’accesso, ogni qualvolta sia costretto ad assentarsi dalla stanza dove è ubicata la propria postazione di lavoro o nel caso ritenga di non essere in grado di presidiare l’accesso alla medesima: lasciare un PC incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

6. Le informazioni archiviate sul PC locale e sugli spazi condivisi della rete devono essere esclusivamente quelle necessarie all’attività lavorativa assegnata.

7. La gestione dei dati sulla propria postazione di lavoro è demandata al dipendente/collaboratore che dovrà provvedere a memorizzare sulle aree delle condivisioni (server) i dati che possono essere utilizzati anche da altri utenti della propria area/ufficio/gruppo, evitando di mantenere l’esclusività su di essi ed in modo da garantire la sicurezza e il salvataggio degli stessi nel caso di eventuali necessità di ripristino della postazione. Non è consentita l’installazione di programmi diversi da quelli autorizzati dall’Amministratore di Sistema.

8. L’Amministratore di Sistema può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosa per la sicurezza dei PC, per la rete locale e server, nonché potrà cambiare tutte le impostazioni eventualmente configurate che possano interferire con il corretto funzionamento dei servizi informatici.

9. È obbligatorio monitorare e consentire l’installazione degli aggiornamenti di sistema che vengono proposti automaticamente, al primo momento disponibile, in modo tale da mantenere la postazione sempre funzionale e protetta.

10. È assolutamente vietato utilizzare la propria postazione di lavoro per l’acquisizione, la duplicazione e/o la trasmissione illegale di opere protette da copyright.

11. È vietato l’utilizzo di supporti di memoria (chiavi USB, CD, DVD o altri supporti) per il salvataggio di dati trattati tramite gli Strumenti, salvo che il supporto utilizzato sia stato fornito dal Responsabile dei Sistemi Informativi. In tale caso, il supporto fornito può essere utilizzato esclusivamente per finalità lavorative.

12. È vietato connettere sulla propria postazione o alla rete locale, qualsiasi dispositivo (PC esterni, router, switch, modem, etc.) o qualsiasi periferica non autorizzata preventivamente dall’Amministratore di Sistema.

13. Nel caso in cui il dipendente/collaboratore dovesse notare comportamenti anomali della propria postazione di lavoro, è tenuto a comunicarlo tempestivamente al Responsabile dei Sistemi Informativi.

I LOG RELATIVI ALL’UTILIZZO DI STRUMENTI, REPERIBILI NELLA MEMORIA DEGLI STRUMENTI STESSI OVVERO SUI SERVER O SUI ROUTER, NONCHÉ I FILE CON ESSI TRATTATI SONO REGISTRATI E POSSONO ESSERE OGGETTO DI CONTROLLO DA PARTE DEL TITOLARE DEL TRATTAMENTO, ATTRAVERSO L’AMMINISTRATORE DI SISTEMA, PER ESIGENZE ORGANIZZATIVE E PRODUTTIVE, PER LA SICUREZZA DEL LAVORO E PER LA TUTELA DEL PATRIMONIO. I CONTROLLI POSSONO AVVENIRE SECONDO LE DISPOSIZIONI PREVISTE AL SUCCESSIVO ART. 12 DEL PRESENTE REGOLAMENTO. LE INFORMAZIONI COSÌ RACCOLTE SONO ALTRESÌ UTILIZZABILI A TUTTI I FINI CONNESSI AL RAPPORTO DI LAVORO, COMPRESA LA VERIFICA DEL RISPETTO DEL PRESENTE REGOLAMENTO, CHE COSTITUISCE ADEGUATA INFORMAZIONE DELLE MODALITÀ D'USO DEGLI STRUMENTI E DI EFFETTUAZIONE DEI CONTROLLI AI SENSI DEL REGOLAMENTO EUROPEO 679/2016 *“GENERAL DATA PROTECTION REGULATION”.*

Art. 8 - Utilizzo di internet

Le regole di seguito specificate sono adottate anche ai sensi delle "Linee guida del Garante per posta elettronica e internet" pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007. Ciascun dipendente /collaboratore si deve attenere alle seguenti regole di utilizzo della rete Internet e dei relativi servizi.

1. È ammessa solo la navigazione in siti considerati correlati con la prestazione lavorativa.

2. È vietato compiere azioni che siano potenzialmente in grado di arrecare danno all'Ente, ad esempio, il download o l'upload di file audio e/o video, l'uso di servizi di rete con finalità ludiche o, comunque, estranee all'attività lavorativa.

3. È vietato a chiunque il download di qualunque tipo di software gratuito (*freeware*) o *shareware* prelevato da siti Internet, se non espressamente autorizzato dal Responsabile dei Sistemi Informatici;

4. L'Ente si riserva di bloccare l'accesso a siti "a rischio" attraverso l'utilizzo di *black list* pubbliche in continuo aggiornamento e di predisporre filtri, basati su sistemi euristici di valutazione del livello di sicurezza dei siti web remoti, tali da prevenire operazioni potenzialmente pericolose o comportamenti impropri. In caso di blocco accidentale di siti di interesse, potrà contattare l'Amministratore di Sistema per uno sblocco selettivo.

5. Nel caso in cui, per ragioni di servizio, si necessiti di una navigazione libera dai filtri, è necessario richiedere lo sblocco mediante una mail indirizzata al Responsabile dei Sistemi informatici, ed in copia alla Direzione Generale per la necessaria autorizzazione, nella quale siano indicati chiaramente: motivo della richiesta, dipendente/collaboratore e postazione da cui effettuare la navigazione libera, intervallo di tempo richiesto per completare l'attività. Il dipendente/collaboratore, nello svolgimento delle proprie attività, deve comunque tenere presente in modo particolare i punti - Controlli sugli Strumenti (art. 6.1 Provv. Garante, ad integrazione dell'Informativa ex art. 13 Reg. 679/2016) e - Conservazione dei dati del presente regolamento. Al termine dell'attività l'Amministratore di Sistema ripristinerà i filtri alla situazione iniziale.

6. È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo i casi direttamente autorizzati dalla Direzione Generale e dall'Amministratore di Sistema, con il rispetto delle normali procedure di acquisto.

7. È assolutamente vietato l'utilizzo di abbonamenti privati per effettuare la connessione a Internet tranne in casi del tutto eccezionali e previa autorizzazione della Direzione Generale.

8. È assolutamente vietata la partecipazione a Forum non professionali, ai Social Network, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

9. È consentito l'uso di eventuali sistemi di messaggistica istantanea, per permettere una efficace e comoda comunicazione tra i colleghi, mediante i soli strumenti autorizzati. Tali sistemi hanno lo scopo di migliorare la collaborazione tra utenti aggiungendo un ulteriore canale comunicativo rispetto agli spostamenti fisici, alle chiamate telefoniche ed e-mail. È consentito un utilizzo legato esclusivamente a scopi professionali. Anche su tali strumenti di messaggistica istantanea è attivo il monitoraggio e la registrazione dell'attività degli utenti, secondo le disposizioni dei punti - Controlli sugli Strumenti (art. 6.1 Provv. Garante, ad integrazione dell'Informativa ex art. 13 Reg. 679/16) e - Conservazione dei dati del presente Regolamento.

10. Per motivi tecnici e di buon funzionamento del sistema informatico è buona norma, salvo comprovata necessità, non accedere a risorse web che impegnino in modo rilevante banda, come a titolo esemplificativo: filmati (tratti da you tube, siti di informazione, siti di streaming ecc) o web radio, in quanto possono limitare e/o compromettere l'uso della rete agli altri utenti.

SI INFORMA CHE L'ENTE, PER IL TRAMITE DELL'AMMINISTRATORE DI SISTEMA, NON EFFETTUA LA MEMORIZZAZIONE SISTEMATICA DELLE PAGINE WEB VISUALIZZATE DAL SINGOLO DIPENDENTE/COLLABORATORE, NÉ CONTROLLA CON SISTEMI AUTOMATICI I DATI DI NAVIGAZIONE DELLO STESSO. SI INFORMA TUTTAVIA CHE AL FINE DI GARANTIRE IL SERVIZIO INTERNET E LA SICUREZZA DEI SISTEMI INFORMATIVI, NONCHÉ PER ESIGENZE ORGANIZZATIVE E PRODUTTIVE, PER LA SICUREZZA DEL LAVORO E PER LA TUTELA PATRIMONIALE, L'ENTE REGISTRA I DATI DI NAVIGAZIONE (FILE DI LOG RIFERITI AL TRAFFICO WEB) CON MODALITÀ INIZIALMENTE VOLTE A PRECLUDERE L'IMMEDIATA E DIRETTA IDENTIFICAZIONE DI UTENTI, MEDIANTE OPPORTUNE AGGREGAZIONI. SOLO IN CASI ECCEZIONALI E DI COMPROVATA URGENZA RISPETTO ALLE FINALITÀ SOPRA DESCRITTE, L'ENTE POTRÀ TRATTARE I DATI DI NAVIGAZIONE RIFERENDOLI SPECIFICATAMENTE AD UN SINGOLO NOME UTENTE. IN TALI CASI I CONTROLLI AVVERRANNO NELLE FORME INDICATE AL SUCCESSIVO PUNTO 12 DEL PRESENTE REGOLAMENTO. LE INFORMAZIONI COSÌ RACCOLTE SONO ALTRESÌ UTILIZZABILI A TUTTI I FINI CONNESSI AL RAPPORTO DI LAVORO, COMPRESA LA VERIFICA DEL RISPETTO DEL PRESENTE REGOLAMENTO, CHE COSTITUISCE ADEGUATA INFORMAZIONE DELLE MODALITÀ D'USO DEGLI STRUMENTI E DI EFFETTUAZIONE DEI CONTROLLI AI SENSI DEL REGOLAMENTO EUROPEO 679/16 "GENERAL DATA PROTECTION REGULATION".

Art. 9 - Utilizzo della posta elettronica

Le regole di seguito specificate sono adottate anche ai sensi delle *"Linee guida del Garante per posta elettronica e internet"* pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007. Ciascun dipendente/collaboratore si deve attenere alle seguenti regole di utilizzo dell'indirizzo di Posta elettronica. Le caselle di posta elettronica rilasciate dall'Ater di Viterbo sono di due tipi:

- caselle di posta elettronica istituzionale e di posta certificata: riconducibili ad un'unità organizzativa;
- casella di posta elettronica individuale: casella assegnata al singolo utente interno.

1. Ad ogni dipendente/collaboratore viene fornito un account e-mail nominativo, generalmente coerente con il modello *nome.cognome@atervt.it.* L'utilizzo dell'e-mail deve essere limitato esclusivamente a scopi lavorativi, ed è assolutamente vietato ogni utilizzo di tipo privato. Il dipendente/collaboratore a cui è assegnata una casella di posta elettronica è responsabile del corretto utilizzo della stessa.

2. L'Ente fornisce, altresì, delle caselle di posta elettronica associate a ciascuna unità organizzativa, area/uffici/gruppi di lavoro il cui utilizzo è da preferire rispetto alle e-mail nominative qualora le comunicazioni siano di interesse collettivo: questo per evitare che degli utenti singoli mantengano l'esclusività su dati.

3. L'iscrizione a *mailing-list* o *newsletter* esterne con l'indirizzo ricevuto è concessa esclusivamente per motivi professionali. Prima di iscriversi occorre verificare anticipatamente l'affidabilità del sito che offre il servizio.

4. Allo scopo di garantire sicurezza alla rete, è assolutamente necessario evitare di aprire messaggi di posta in arrivo da mittenti di cui non si conosce l'identità o con contenuto sospetto o insolito, oppure che contengano allegati di tipo *.exe, *.com, *.vbs, *.htm, *.scr, *.bat, *.js e *.pif. È necessario porre molta attenzione, inoltre, alla credibilità del messaggio e del mittente per evitare casi di *phishing* o frodi informatiche. In qualunque situazione di incertezza contattare il Responsabile dei Sistemi Informatici per una valutazione dei singoli casi.

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

6. Nel caso fosse necessario inviare allegati "pesanti" (fino a 10 MB) è opportuno ricorrere prima alla compressione dei file originali in un archivio di formato .zip o equivalenti. Nel caso di allegati ancora più voluminosi è necessario rivolgersi al Responsabile dei Sistemi Informativi.

7. Nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati personali o dati personali sensibili, è obbligatorio che questi allegati vengano preventivamente resi inintelligibili attraverso crittazione con apposito software (archiviazione e compressione con password). La password di crittazione deve essere comunicata al destinatario attraverso un canale diverso dalla mail (ad esempio per lettera o per telefono) e mai assieme ai dati criptati. Tutte le informazioni, i dati personali e/o sensibili di competenza, possono essere inviati soltanto a destinatari - persone o Enti - qualificati e competenti.

8. Non è consentito l'invio automatico di e-mail all'indirizzo e-mail privato (attivando per esempio un "inoltro" automatico delle e-mail entranti), anche durante i periodi di assenza (es. ferie, malattia, infortunio ecc.). In questa ultima ipotesi, è raccomandabile utilizzare un messaggio "*Out of Office*" facendo menzione di chi, all'interno dell'Ente, assumerà le mansioni durante l'assenza, oppure indicando un indirizzo di mail alternativo preferibilmente di tipo collettivo, tipo *info@atervt.it*, rivolgersi al Responsabile dei Sistemi Informatici per tale eventualità.

9. In caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, qualora non fosse possibile attivare la funzione *autoreply* o l'inoltro automatico su altre caselle e si debba conoscere il contenuto dei messaggi di posta elettronica, il titolare della casella di posta ha la facoltà di delegare un altro dipendente (fiduciario) per verificare il contenuto di messaggi e per inoltrare al Titolare del trattamento, quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Sarà compito del Dirigente responsabile assicurarsi che sia redatto un verbale attestante quanto avvenuto e che si sia informato il lavoratore interessato alla prima occasione utile;

10. La diffusione massiva di messaggi di posta elettronica deve essere effettuata esclusivamente per motivi inerenti il servizio, solo su autorizzazione del Responsabile dell'ufficio/area competente. Per evitare che le eventuali risposte siano inoltrate a tutti, generando traffico eccessivo ed indesiderato, i destinatari dovranno essere messi in copia nascosta (Bcc o Ccn) se la tipologia del messaggio lo consente.

11. È vietato inviare messaggi di posta elettronica in nome e per conto di un altro dipendente/collaboratore, salvo sua espressa autorizzazione;

12. La casella di posta elettronica personale deve essere mantenuta in ordine, cancellando messaggi e documenti la cui conservazione non è più necessaria. Anche la conservazione di messaggi con allegati pesanti è da evitare per quanto possibile, preferendo, in alternativa, il salvataggio dell'allegato sulle condivisioni.

13. I messaggi in entrata vengono sistematicamente analizzati alla ricerca di virus e malware e per l'eliminazione dello spam. I messaggi che dovessero contenere virus vengono eliminati dal sistema e il mittente/destinatario viene avvisato mediante messaggio specifico.

SI INFORMA CHE, AI SENSI DELLA NORMATIVA SULL'ARCHIVIAZIONE E CONSERVAZIONE DEGLI ATTI AMMINISTRATIVI, DELL'ARTICOLO 2214 DEL CODICE CIVILE E DELL'ARTICOLO 22 DEL DPR 600/73, PER OTTEMPERARE LEGITTIME ISTANZE DI ACCESSO AGLI ATTI AI SENSI DELLA L. 241/90 O ACCESSO CIVICO GENERALIZZATO (D. LGS 33/13) L'ENTE DEVE CONSERVARE PER DIECI ANNI SUI PROPRI SERVER DI POSTA ELETTRONICA TUTTI I MESSAGGI DI POSTA ELETTRONICA AVENTI RILEVANZA ISTRUTTORIA O INERENTI L 'ATTIVITÀ PROCEDIMENTALE E CONTRATTUALE. L'ENTE, PER IL TRAMITE DELL'AMMINISTRATORE DI SISTEMA, NON CONTROLLA SISTEMATICAMENTE IL FLUSSO DI COMUNICAZIONI MAIL NÉ È DOTATO DI SISTEMI PER LA LETTURA O ANALISI SISTEMATICA DEI MESSAGGI DI POSTA ELETTRONICA OVVERO DEI RELATIVI DATI ESTERIORI, AL DI LÀ DI QUANTO TECNICAMENTE NECESSARIO PER SVOLGERE IL SERVIZIO E-MAIL. TUTTAVIA, IN CASO DI ASSENZA IMPROVVISA O PROLUNGATA DEL DIPENDENTE OVVERO PER IMPRESCINDIBILI ESIGENZE ORGANIZZATIVE E PRODUTTIVE, PER LA SICUREZZA DEL LAVORO E PER LA TUTELA DEL PATRIMONIO, L'ENTE PER IL TRAMITE DELL'AMMINISTRATORE DI SISTEMA PUÒ, SECONDO LE PROCEDURE INDICATE SUCCESSIVO ART. 12 DEL PRESENTE REGOLAMENTO, ACCEDERE ALL'ACCOUNT DI POSTA ELETTRONICA, PRENDENDO VISIONE DEI MESSAGGI, SALVANDO O CANCELLANDO FILE. IN CASO DI CESSAZIONE DEL RAPPORTO LAVORATIVO, LA MAIL AFFIDATA ALL'INCARICATO VERRÀ SOSPESA PER UN PERIODO MASSIMO DI 6 MESI E SUCCESSIVAMENTE DISATTIVATA. NEL PERIODO DI SOSPENSIONE L'ACCOUNT RIMARRÀ ATTIVO E VISIBILE AD UN SOGGETTO INCARICATO DALL'ENTE SOLO IN RICEZIONE, CHE TRATTERÀ I DATI E LE INFORMAZIONI PERVENUTE PER ESIGENZE ORGANIZZATIVE E PRODUTTIVE (AD ESEMPIO PER NON PERDERE COMUNICAZIONI RELATIVE A PROCEDIMENTI IN ESSERE, A RICHIESTE INERENTI L'UFFICIO O L'ENTE, ISTANZE, DICHIARAZIONI ECC.), PER LA SICUREZZA DEL LAVORO E PER LA TUTELA DEL PATRIMONIO, TRASMETTENDONE IL CONTENUTO AD ALTRI DIPENDENTI (SE IL MESSAGGIO HA CONTENUTO LAVORATIVO) OVVERO CANCELLANDOLO (SE IL MESSAGGIO NON HA CONTENUTO LAVORATIVO). IL SOGGETTO INCARICATO NON RISPONDERÀ MAI USANDO L'ACCOUNT SOSPESO E IL SISTEMA IN OGNI CASO GENERERÀ UNA RISPOSTA AUTOMATICA AL MITTENTE, INVITANDOLO A REINVIARE IL MESSAGGIO AD ALTRO INDIRIZZO MAIL.

A RICHIESTA SCRITTA DEL DIPENDENTE, VERRÀ MESSO A SUA DISPOSIZIONE L'ACCOUNT SOSPESO PER PERMETTERE L'ESTRAZIONE DI EVENTUALI CONTENUTI CHE, NONOSTANTE L'ESPRESSO ED ESPLICITO DIVIETO DI USO DELLO STRUMENTO PER FINALITÀ DIVERSE DA QUELLE LAVORATIVE, DOVESSERO ESSERE PRESENTI. IN OGNI CASO SI INFORMA CHE IL CONTENUTO DELLA MAILBOX OGGETTO DI SOSPENSIONE POTRÀ ESSERE TRATTATO DALL'ENTE, PER IL TRAMITE DELL'AMMINISTRATORE DI SISTEMA, PER ESIGENZE ORGANIZZATIVE E PRODUTTIVE, PER LA SICUREZZA DEL LAVORO E PER LA TUTELA DEL PATRIMONIO. LE INFORMAZIONI COSÌ RACCOLTE SARANNO UTILIZZABILI A TUTTI I FINI CONNESSI AL RAPPORTO DI LAVORO, COMPRESA LA VERIFICA DEL RISPETTO DEL PRESENTE REGOLAMENTO, CHE COSTITUISCE ADEGUATA INFORMAZIONE DELLE MODALITÀ D'USO DEGLI STRUMENTI E DI EFFETTUAZIONE DEI CONTROLLI AI SENSI DEL REGOLAMENTO EUROPEO 679/2016 "GENERAL DATA PROTECTION REGULATION".

Art. 10 - Utilizzo dei telefoni, fax, fotocopiatrici, scanner e stampanti

Il dipendente è consapevole che gli Strumenti di stampa, così come anche il telefono, sono di proprietà dell'Ente e sono resi disponibili al dipendente/collaboratore per rendere la prestazione lavorativa. Pertanto ne viene concesso l'uso esclusivamente per tale fine.

1. Il telefono fisso affidato al dipendente/collaboratore è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa e non sono quindi consentite comunicazioni a carattere personale e/o non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di comunicazioni a carattere personale è consentito solo nel caso di comprovata necessità ed urgenza.

2. Qualora venisse assegnato un cellulare al dipendente/collaboratore, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Ai cellulari e smartphone si applicano le medesime regole sopra previste per gli altri dispositivi informatici (cfr. - Utilizzo degli Strumenti elettronici (PC, notebook e altri strumenti con relativi software e applicativi) "Utilizzo di personal computer"), per quanto riguarda il mantenimento di un adeguato livello di sicurezza informatica. In particolare si raccomanda il rispetto delle regole per una corretta navigazione in Internet (cfr. 8), se consentita.

3. Per gli smartphone è vietata l'installazione e l'utilizzo di applicazioni (o altresì denominate "app" nel contesto degli smartphone) diverse da quelle autorizzate dall'Amministratore di Sistema.

4. È vietato l'utilizzo dei fax per fini personali, tanto per spedire quanto per ricevere documentazione, fatta salva esplicita autorizzazione da parte del Responsabile dell'ufficio/area competente.

5. È vietato l'utilizzo delle fotocopiatrici per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile dell'ufficio/area competente.

6. Per quanto concerne l'uso delle stampanti gli utenti sono tenuti a:

- stampare documenti solo se strettamente necessari per lo svolgimento delle proprie funzioni operative;
- prediligere le stampanti di rete condivise, rispetto a quelle locali/personali, per ridurre l'utilizzo di materiali di consumo (toner ed altri consumabili);
- prediligere la stampa in bianco/nero e fronte/retro al fine di ridurre i costi, se possibile.

7. Le stampanti e le fotocopiatrici devono essere spente ogni sera prima di lasciare gli uffici o in caso di inutilizzo prolungato.

8. Nel caso in cui si rendesse necessaria la stampa di informazioni riservate il dipendente/collaboratore dovrà presidiare il dispositivo di stampa per evitare la possibile perdita o divulgazione di tali informazioni e persone terze non autorizzate.

Art. 11 - Assistenza agli utenti e manutenzioni

1. L'Amministratore di Sistema può accedere ai dispositivi informatici sia direttamente, sia mediante software di accesso remoto installato sui dispositivi, per i seguenti scopi:

- verifica e risoluzione di problemi sistemistici ed applicativi, su segnalazione dell'utente finale;
- verifica del corretto funzionamento dei singoli dispositivi in caso di problemi rilevati nella rete;
- richieste di aggiornamento software e manutenzione preventiva hardware e software.

2. Tutti gli interventi tecnici possono essere richiesti al Responsabile dei Sistemi Informatici attraverso la casella *ced@atervt.it*, o eventuale software dedicato messo a disposizione l'Amministratore di Sistema, possono avvenire previo consenso del dipendente/collaboratore quando l'intervento stesso richiede l'accesso ad aree personali del dipendente/collaboratore stesso. Qualora l'intervento tecnico in loco o in remoto non necessiti di accedere mediante credenziali utente, l'Amministratore di Sistema è autorizzato ad effettuare gli interventi senza il consenso del dipendente/collaboratore cui la risorsa è assegnata.

3. L'accesso in teleassistenza sui PC della rete richiesto da terzi (fornitori e/o altri) deve essere richiesto al Responsabile dei Sistemi Informatici e autorizzato dall'Amministratore di Sistema, per le verifiche delle modalità di intervento per il primo accesso. Le richieste successive, se effettuate con la medesima modalità, possono essere gestite autonomamente dall'utente finale. Durante gli interventi in teleassistenza da parte di operatori terzi, il dipendente/collaboratore richiedente o Responsabile dei Sistemi Informatici devono presenziare la sessione remota, in modo tale da verificare ed impedire eventuali comportamenti non conformi al presente Regolamento.

12 - Controlli sugli Strumenti (art. 6.1 Provv. Garante, ad integrazione dell'Informativa ex art. 13 Reg. 679/2016)
Poiché in caso di violazioni contrattuali e giuridiche, sia il datore di lavoro, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'Ente verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico. Il datore di lavoro, infatti, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori (art. 4, comma 2), di sistemi che consentono indirettamente il controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori.

1. I controlli devono essere effettuati nel rispetto dell'art. 3 del presente Regolamento e dei seguenti principi:
   - **Proporzionalità:** il controllo e l'estensione dello stesso dovrà rivestire, in ogni caso, un carattere adeguato, pertinente e non eccessivo rispetto alla/alle finalità perseguite, ma resterà sempre entro i limiti minimi.
   - **Trasparenza:** l'adozione del presente Regolamento ha l'obiettivo di informare gli utenti sui diritti ed i doveri di entrambe le parti.
   - **Pertinenza e non eccedenza:** ovvero evitando un'interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, così come la possibilità di controlli prolungati, costanti o indiscriminati.

2. L'uso degli Strumenti Informatici dell'Ente può lasciare traccia delle informazioni sul relativo uso, come analiticamente spiegato nei riquadri di cui agli artt. 6 - 7 - 8 - 9 del presente Regolamento. Tali informazioni, che possono contenere dati personali eventualmente anche sensibili del dipendente/collaboratore, possono essere oggetto di controlli da parte dell'Ente, per il tramite dell'Amministratore di Sistema, volti a garantire esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio, nonché per la sicurezza e la salvaguardia del sistema informatico, per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento / sostituzione / implementazione di programmi, manutenzione hardware, etc.). Gli interventi di controllo sono di due tipi (di seguito descritti) e possono permettere all'Ente di prendere indirettamente cognizione dell'attività svolta con gli Strumenti.

3. Controlli per la tutela del patrimonio, nonché per la sicurezza e la salvaguardia del sistema informatico. Controlli per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, ecc.). Qualora per le finalità qui sopra descritte risulti necessario l'accesso agli Strumenti e alle risorse informatiche e relative informazioni descritte agli artt. 6 - 7 - 8 - 9, l'Amministratore di Sistema si atterrà al processo descritto qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo):
   i. Avviso generico a tutti i dipendenti della presenza di comportamenti anomali che possono mettere a rischio la sicurezza del sistema informativo e richiamo all'esigenza di attenersi al rispetto del presente Regolamento.
   ii. Successivamente, dopo almeno 7 giorni, se il comportamento anomalo persiste, l'Ente potrà autorizzare il personale addetto al controllo, potendo così accedere alle informazioni descritte ai punti 6 - 7 - 8 - 9, con possibilità di rilevare files trattati, siti web visitati, software installati, documenti scaricati, statistiche sull'uso di risorse ecc. nel corso dell'attività lavorativa. Tale attività potrà essere effettuata in forma anonima ovvero tramite controllo del numero IP, dell'Utente e con l'identificazione del soggetto che non si attiene alle istruzioni impartite.

iii. Qualora il rischio di compromissione del sistema informativo sia imminente e grave a tal punto da non permettere l'attesa dei tempi necessari per i passaggi procedimentali descritti ai punti 1 e 2, l'Amministratore di Sistema potrà intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia.

Art. 13 - Controlli per esigenze produttive e di organizzazione

Per esigenze produttive e di organizzazione si intendono, fra le altre, l'urgente ed improrogabile necessità di accedere a files o informazioni lavorative di cui si è ragionevolmente certi che siano disponibili su risorse informatiche di un dipendente/collaboratore (quali file salvati, posta elettronica, chat, SMS, ecc) che non sia reperibile, in quanto ad esempio assente, temporaneamente irreperibile ovvero cessato.

1. Qualora per queste finalità, risulti necessario l'accesso alle risorse informatiche e relative informazioni descritte ai punti 6 - 7 - 8 - 9, l'Amministratore di Sistema si atterrà alla procedura descritta qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo):

i. Redazione di un atto da parte del Direttore Generale e/o Responsabile dei Sistemi Informatici che comprovi le necessità produttive e di organizzazione che richiedano l'accesso allo Strumento.

ii. Incarico all'Amministratore di sistema di accedere alla risorsa con credenziali di Amministratore ovvero tramite l'azzeramento e la contestuale creazione di nuove credenziali di autenticazione del dipendente/collaboratore interessato, con avviso che al primo accesso alla risorsa, lo stesso dovrà inserire nuove credenziali.

iii. Redazione di un verbale che riassuma i passaggi precedenti.

iv. In ogni caso l'accesso ai documenti presenti nella risorsa è limitato a quanto strettamente indispensabile alle finalità produttive e di organizzazione del lavoro.

v. Qualora indirettamente si riscontrino file o informazioni anche personali, esse potranno essere altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, considerato che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo 679/2016 "*General Data Protection Regulation"*.

TUTTI I CONTROLLI SOPRA DESCRITTI AVVENGONO NEL RISPETTO DEL PRINCIPIO DI NECESSITÀ E NON ECCEDENZA RISPETTO ALLE FINALITÀ DESCRITTE NEL PRESENTE REGOLAMENTO. DELL'ATTIVITÀ SOPRA DESCRITTA VIENE REDATTO VERBALE SOTTOSCRITTO DALL'AMMINISTRATORE DI SISTEMA CHE HA SVOLTO L'ATTIVITÀ. IN CASO DI NUOVO ACCESSO DA PARTE DELL'UTENTE ALLO STRUMENTO INFORMATICO OGGETTO DI CONTROLLO, LO STESSO DOVRÀ AVVENIRE PREVIO RILASCIO DI NUOVE CREDENZIALI (SALVO DIVERSE ESIGENZE TECNICHE). QUALORA INDIRETTAMENTE SI RISCONTRINO FILE O INFORMAZIONI ANCHE PERSONALI, ESSE POTRANNO ESSERE ALTRESÌ UTILIZZABILI A TUTTI I FINI CONNESSI AL RAPPORTO DI LAVORO, CONSIDERATO CHE IL PRESENTE REGOLAMENTO COSTITUISCE ADEGUATA INFORMAZIONE DELLE MODALITÀ D'USO DEGLI STRUMENTI E DI EFFETTUAZIONE DEI CONTROLLI, SEMPRE NEL RISPETTO DI QUANTO DISPOSTO DAL REGOLAMENTO EUROPEO 679/2016 *"GENERAL DATA PROTECTION REGULATION".*

Art.14 - Acquisto di hardware e software

Tutto l'hardware ed il software potrà essere acquistato solo previa richiesta di parere tecnico favorevole da parte del Responsabile dei Sistemi Informativi, che controllerà le richieste di acquisto al fine di valutare la compatibilità tecnica con l'infrastruttura informatica aziendale e l'idoneità dei prodotti richiesti alle normative stabilite dell'Agenzia per l'Italia Digitale (AgID). Nel caso in cui gli strumenti proposti non possano, per ragioni tecniche, essere installati, saranno individuate, ove possibile e nel limite della tecnologia, soluzioni alternative, tecnicamente fattibili, d'intesa con il Responsabile dell'ufficio/area richiedente. I supporti originali dei software acquistati e le relative licenze devono essere conservati presso il Responsabile dei Sistemi Informativi, così da consentire le operazioni di verifica della disponibilità di licenze e l'eventuale reinstallazione delle procedure.

Art. 15 - Conservazione dei dati

1. In riferimento agli articoli 5 e 6 del Reg. 679/2016 e in applicazione ai principi di diritto di accesso, legittimità, proporzionalità, sicurezza ed accuratezza e conservazione dei dati, le informazioni relative all'accesso ad Internet e dal traffico telematico (log di sistema e del server proxy), la cui conservazione non sia necessaria, saranno cancellati entro dodici mesi dalla loro produzione.

2. In casi eccezionali – ad esempio: per esigenze tecniche o di sicurezza; o per l'indispensabilità dei dati rispetto all'esercizio o 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 – è consentito il prolungamento dei tempi di conservazione limitatamente al soddisfacimento delle esigenze sopra esplicitate.

3. L'Ente si impegna ad applicare le misure di sicurezza nel trattamento e nella conservazione di tale tipologia di dati alla luce di quanto stabilito dal Legislatore.

Art. 16 - Partecipazioni a Social Media

1. L'utilizzo a fini promozionali e commerciali di Facebook, Twitter, Linkedin, dei blog e dei forum, anche professionali, (ed altri siti o social media) è gestito ed organizzato esclusivamente dall'Ente attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti o collaboratori.

2. Fermo restando il diritto della persona alla libertà di espressione, l'Ente ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine ed il patrimonio, anche immateriale, quanto i propri collaboratori, i propri clienti e fornitori, gli altri partners, oltre che gli stessi utenti utilizzatori dei social media, fermo restando che è vietata la partecipazione agli stessi social media durante l'orario di lavoro.

3. Il presente articolo deve essere osservato dal dipendente/collaboratore sia che utilizzi dispositivi messi a disposizione dall'Ente, sia che utilizzi propri dispositivi, sia che partecipi ai social media a titolo personale, sia che lo faccia per finalità professionali, come dipendente dell'Ente.

4. La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni considerate dall'Ente riservate ed in genere, a titolo esemplificativo e non esaustivo, sulle informazioni inerenti attività, dati contabili, finanziari, progetti, procedimenti svolti o in svolgimento presso gli uffici. Inoltre, ogni comunicazione e divulgazione di contenuti dovrà essere effettuata nel pieno rispetto dei diritti di proprietà industriale e dei diritti d'autore, sia di terzi che dell'Ente. Il dipendente/collaboratore, nelle proprie comunicazioni, non potrà quindi inserire il nominativo e il logo dell'Ente, né potrà pubblicare disegni, modelli od altro connesso ai citati diritti. Ogni deroga a quanto sopra disposto potrà peraltro avvenire solo previa specifica autorizzazione della Direzione Generale.

5. Il dipendente/collaboratore deve garantire la tutela della riservatezza e dignità delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi e in genere di collaboratori, se non con il preventivo personale consenso di questi, e comunque non potrà postare nei social media immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro dell'Ater di Viterbo, se non con il preventivo consenso del proprio Responsabile dell'ufficio/area.

6. Qualora il dipendente/collaboratore intenda usare social network, blog, forum su questioni anche indirettamente professionali (es. post su prodotti, servizi, fornitori, partner, ecc.) egli esprimerà unicamente le proprie opinioni personali; pertanto, ove necessario od opportuno per la possibile connessione con l'Ente, in particolare in forum professionali, il dipendente/collaboratore dovrà precisare che le opinioni espresse sono esclusivamente personali e non riconducibili all'Ente.

Art. 17 - Pubblicazione e messa a disposizione

1. Il presente Regolamento è stato redatto dal Responsabile dei Sistemi Informatici con il supporto del DPO e la consulenza dell'Amministratore di Sistema che è chiamato a garantire l'adeguamento degli adempimenti.

2. La sua pubblicizzazione, a cura del Responsabile dei Sistemi Informativi, avverrà nelle seguenti forme: trasmissione per posta elettronica attraverso la rete informatica interna, mediante affissione nei luoghi di lavoro con modalità analoghe a quelle previste dall'art. 7 dello Statuto dei lavoratori e pubblicazione nella relativa area dedicata all'Amministrazione Trasparente del sito istituzionale.

Art. 18 - Sanzioni disciplinari

È fatto obbligo a tutti i dipendenti/collaboratori/utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento. Eventuali violazioni del presente Regolamento da parte dei dipendenti a seconda della gravità della infrazione, comportano l'adozione di provvedimenti così come previsto dai Regolamenti aziendali riferiti alla gestione del personale nonché dal CCNL Federcasa. Rimane comunque riservato il diritto di intraprendere azioni civili e penali nei confronti dei responsabili di qualsivoglia violazione a danno dell'Ente.

Art.19 - Aggiornamento e revisione

Il presente Regolamento è soggetto a revisione periodica. Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni o modifiche al presente Regolamento tramite comunicazione alla Direzione Aziendale.