Unione Rubicone e Mare

UNIONE RUBICONE E MARE
Provincia di Forlì – Cesena

REGOLAMENTO SULL'UTILIZZO E LA GESTIONE DELLE RISORSE INFORMATICHE DELL'ENTE. Regole di condotta ed obblighi degli autorizzati del trattamento dei dati personali, in relazione all'uso degli strumenti informatici, di Internet e della Posta Elettronica.

Sommario

1 Premessa

La crescente diffusione delle nuove tecnologie informatiche e, in particolare, l'utilizzo massiccio e quasi esclusivo delle tecnologie ICT nell'attività lavorativa dell'Ente, oltre che il libero accesso alla rete internet dai diversi dispositivi informatici, espongono l'Ente e gli Utenti (come definiti all'art. 1.4 del presente manuale) a rischi e responsabilità conseguenti alla violazione di specifiche disposizioni normative creando un potenziale pregiudizio alle funzioni organizzative, alla sicurezza e all'immagine dell'Amministrazione.
Considerato che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, i comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro e tutte le risorse ICT (Information and Communication Technology) fornite dall'Amministrazione agli Utenti devono essere utilizzate in modo appropriato, efficiente, rispettoso e unicamente per motivi lavorativi, l'Ente adotta il presente Manuale interno al fine di evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza informatica e al trattamento dei dati.
Considerato, inoltre, che l'Ente, nell'ottica di uno svolgimento più agevole della propria attività, mette a disposizione dei propri collaboratori che ne necessitano per il tipo di funzioni svolte, dispositivi informatici e di comunicazione in genere (computer portatili, tablet, telefoni cellulari, smartphone, etc.), sono state inserite nel presente Manuale alcune clausole relative alle modalità e ai doveri che ciascun collaboratore, ovvero ciascun Utente, deve osservare nell'utilizzo di detta strumentazione.

1.1 Definizione delle risorse ICT

Le risorse ICT, messe a disposizione dall'Ente, oggetto di tutela da parte del presente Manuale, sono:

- il patrimonio informativo di cui all'art. 3 del presente Manuale, detenuto dall'Ente, in formato elettronico;
- i servizi informatici erogati dall'Ente;
- le postazioni di lavoro "fisse" (PC desktop e simili) e "mobili" (PC portatili e simili);
- i dispositivi portatili (smartphone, tablet, etc.);
- i sistemi e i canali di comunicazione (e-mail, PEC, connessione ad internet, social network);
- i dispositivi di stampa;
- i dispositivi per l'elaborazione e l'archiviazione centralizzata dei dati;
- le risorse attive in rete e tutto il materiale hardware in generale;
- le risorse software (Sistemi Operativi, programmi applicativi e simili).

1.2 Finalità del presente documento

Il presente documento si prefigge di dettare le regole per la tutela delle risorse ICT dell'Ente e di fornire, conseguentemente, le indicazioni vincolanti per gli Utenti circa il corretto ed appropriato uso delle stesse. L'Amministrazione, in particolare, intende perseguire i seguenti obiettivi:

- ridurre i rischi relativi alle minacce di sicurezza informatica, preservando la disponibilità, integrità e riservatezza dei dati e la continuità dei servizi erogati;
- garantire il rispetto della normativa in materia.

1.3 Contesto Normativo di riferimento

Il presente Documento fa riferimento al seguente quadro normativo:

- "Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE", che sarà direttamente applicabile in tutti gli Stati dell'Unione Europea a partire dal 25 maggio 2018 (d'ora in poi "GDPR");
- D.Lgs. 196/2003 "Codice della Privacy" (come modificato dal Decreto di adeguamento della normativa nazionale ai principi del GDPR - D.Lgs n. 101/18)";
- Provvedimenti del Garante per la protezione dei dati personali in materia di "misure di sicurezza", in particolare con riguardo agli Amministratori di Sistema (Provvedimento generale del 27.11.2008), come modificato con successivo Provvedimento Generale del 25.06.2009;
- Circolare dell'Agenzia per l'Italia Digitale (AgID) n. 2/2017 del 18 aprile 2017 (GU Serie Generale n. 103 del 05.05.2017) Misure Minime di Sicurezza per le Pubbliche Amministrazioni (MMS-PA);
- Garante della privacy "Linee guida per posta elettronica e internet" del 01.03.2007;
- Direttiva n. 2/2009 del Dipartimento Funzione Pubblica ad oggetto "Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro".

1.4 Ambito di applicazione del presente Manuale

Il presente Manuale si applica ai soggetti di seguito indicati e, per brevità, definiti "Utenti":

a) personale dipendente, a qualsiasi titolo prestante la propria attività in favore dell'Ente, senza distinzione di ruolo e/o livello;
b) consulenti e collaboratori dell'Ente, a prescindere dal rapporto contrattuale intrattenuto con lo stesso;
c) dipendenti e collaboratori di società che hanno un contratto in essere con l'Ente e che utilizzano risorse ICT dello stesso;
d) ospiti dell'Ente, per l'eventuale uso delle risorse ICT dello stesso;
e) altri Enti e/o Agenzie attestati all'interno della rete Intranet dell'Ente, per quanto applicabile.

Le prescrizioni tecnico/organizzative, essendo destinate a disciplinare sia il comportamento di Utenti "meri utilizzatori" (fruitori di PC desktop, smartphone, PC portatili, ecc.), sia il comportamento di Utenti che svolgono mansioni tecniche (Amministratori di Sistema, Amministratori di Rete, gestori di banche dati, gestori di servizi, etc.), si rivolgono alle differenti categorie di soggetti.
Ciascun Utente, in base al proprio profilo "base" o "evoluto", dovrà attuare le norme che sono allo stesso indirizzate e, nel caso di dubbi di applicazione delle stesse, dovrà rivolgersi al Responsabile dei Servizi Informativi (d'ora in poi RSI), ovvero all'Amministratore del Sistema Informatico (d'ora in poi ADS) dell'Ente o al Settore Sistemi Informativi Associati (d'ora in poi SIA).
Mail di contatto: helpdesk@unionerubiconemare.it

2 Regole per il corretto uso delle risorse ICT

2.1 Premessa

Le regole sono declinate su tre versanti: organizzativo, tecnologico-procedurale e comportamentale.
Tutti gli interventi sono finalizzati a garantire la riservatezza, l'integrità e la disponibilità delle

informazioni (dati) di cui l'Ente è Titolare.
In particolare:

- la confidenzialità o riservatezza riguarda la conoscibilità e fruibilità delle informazioni ai soli soggetti autorizzati;
- l'integrità è relativa alla completezza ed inalterabilità delle informazioni;
- la disponibilità concerne l'accessibilità ed usabilità delle informazioni nel tempo da parte dei soggetti autorizzati.

2.2 Soluzioni organizzative

Ciascun Responsabile del trattamento interloquisce direttamente con il RSI, ovvero con l'ADS dell'Ente circa le questioni correlate all'applicazione della normativa di settore con espresso riferimento alle attività di trattamento eseguite mediante strumenti e sistemi automatizzati e più in generale mediante il sistema informativo dell'Ente.

2.2.1 Gestione degli incidenti e databreach

Ogni incidente (ad es. malfunzionamento di PC, indisponibilità dei servizi applicativi e di rete o che più gravemente riguardi il patrimonio di dati e informazioni di cui l'Ente è titolare) deve essere segnalato dall'Utente in modo tempestivo al RSI e all'ADS, che raccoglieranno le segnalazioni e avvieranno il relativo processo di classificazione e risoluzione dell'incidente medesimo al fine di minimizzare gli eventuali impatti negativi sul normale svolgimento delle attività lavorative. Nell'ipotesi in cui la segnalazione dovesse essere formulata da un Utente che non ricopre incarico di Responsabile del trattamento dei dati, la segnalazione stessa dovrà essere formulata per via gerarchica al proprio Responsabile e contestualmente al RSI e all'ADS.

2.2.2 Autenticazione Utenti

L'accesso a tutti i servizi informatici erogati dall'Ente, nonché alle postazioni di lavoro, deve avvenire previa procedura di autenticazione.
Tutti i dipendenti (o assimilabili come tali ai sensi dell'art. 1.4 del presente manuale) dell'Ente devono infatti essere dotati di credenziali di autenticazione al sistema informatico.
La creazione iniziale dell'utente viene eseguita o richiesta dal Settore Personale ed Organizzazione che ne dà comunicazione all'ADS, le successive profilazioni e abilitazioni a specifiche piattaforme o accesso a Banche Dati devono essere richieste formalmente dal Responsabile dell'Utente inviando una mail a helpdesk@unionerubiconemare.it. Gli Utenti riceveranno delle credenziali di autenticazione individuali (composte da nome utente e password), che devono essere mantenute riservate e custodite con cura.
Le utenze devono essere nominative e riconducibili ad una sola persona.
Le credenziali non utilizzate da almeno tre mesi possono essere automaticamente disabilitate dal sistema o dall'ADS senza previa comunicazione agli interessati, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
Le password sono un metodo di autenticazione assegnato dall'Ente per garantire l'accesso protetto ad uno strumento hardware, oppure ad un applicativo software, ovvero ad una banca dati.
La prima caratteristica di una password è la segretezza, e cioè il fatto che non venga svelata ad altri soggetti.
La divulgazione delle proprie password o la trascuratezza nella loro conservazione può causare gravi danni al proprio lavoro, a quello dei colleghi e all'Ente nel suo complesso. Nel tempo, anche la password più sicura perde la sua segretezza. Per questo motivo è buona norma cambiarle con una certa frequenza (password aging).

A questo proposito, diventa necessario gestire il processo di autenticazione informatica, processo attraverso il quale viene verificata l'identità di un Utente che vuole accedere ad un computer, ad un sistema informativo o ad una rete, tramite un sistema automatizzato e con gestione centralizzata (tipo Active Directory di Windows e simili).
Ciascun Utente, da parte sua, per una corretta e sicura gestione delle proprie password, deve rispettare le regole seguenti:

1. le password sono assolutamente personali e non vanno mai comunicate ad altri;
2. occorre cambiare immediatamente una password, al momento del primo accesso al sistema informatico e non appena si abbia alcun dubbio che sia diventata poco “sicura”;
3. le password devono essere lunghe almeno 8 caratteri e devono rispettare almeno 3 dei seguenti criteri: lettere minuscole, lettere maiuscole, caratteri speciali, numeri;
4. le password non devono essere memorizzate su alcun tipo di supporto, quali, ad esempio, Post-It (sul monitor o sotto la tastiera) o agende (cartacee, posta elettronica, telefono cellulare);
5. le password devono essere sostituite almeno ogni 90 giorni, a prescindere dall’esistenza di un sistema automatico di richiesta di cambio password;
6. le password già utilizzate non devono essere riutilizzate a breve distanza di tempo (password history);
7. le password non devono contenere riferimenti esplicitamente riconducibili all’Utente ed al suo username;
8. utilizzare password diverse , differenziate tra servizi ad uso interno (gestionali, mail, ecc.) e piattaforme esterne (siti web, piattaforme web fornite da altri, ecc.) e in particolare non si dovranno utilizzare le stesse password che si utilizzano per i servizi lavorativi su servizi personali (mail personali, social, etc);
9. evitare di digitare la propria password in presenza di altri soggetti che possano vedere la tastiera, anche se collaboratori o dipendenti dell’Ente. In alcuni casi, sono implementati meccanismi che consentono all’Utente un numero limitato di tentativi errati di inserimento della password, oltre ai quali il tentativo di accesso viene considerato un attacco al sistema e l’account viene bloccato.
10. Le regole su elencate sono da considerarsi un punto di partenza, ma non vanno intese come principi cristallizzati nel tempo, valevoli per sempre, perciò occorre mantenersi sempre informati, per esempio, visitando periodicamente il sito dell’autorità “Garante per la protezione dei dati personali” in cui è presente una sezione https://www.garanteprivacy.it/temi/cybersecurity/password contenente una selezione di contenuti in costante aggiornamento, raccolti in un vademecum, “Suggerimenti per creare e gestire password a prova di privacy” https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4248578 con finalità divulgative, tenuto aggiornato in base in base agli sviluppi tecnologici e normativi.

2.2.3 Operazioni a protezione della postazione di lavoro

Di seguito vengono descritte le operazioni a carico dell’Utente e il quadro di riferimento generale per l’esecuzione di operazioni a protezione della propria postazione di lavoro, nel rispetto della sicurezza e dell’integrità del patrimonio di dati e informazioni di cui l'Ente è Titolare.

1. Login e Logout - Il “Login” è l’operazione con la quale l’Utente si connette al sistema informativo dell’Ente o ad una parte di esso, inserendo le proprie credenziali di autenticazione (nome utente e password), aprendo una sessione di lavoro. In molti casi è necessario effettuare più login, tanti quanti sono gli ambienti di lavoro (ad es. applicativi gestionali, Intranet, etc.), ognuno dei quali richiede un nome utente e una password. Il

"Logout" è l'operazione con cui viene chiusa la sessione di lavoro. Al termine della giornata lavorativa, tutte le applicazioni devono essere chiuse secondo le regole previste dall'applicazione stessa. La non corretta chiusura può provocare una perdita di dati o l'accesso agli stessi da parte di persone non autorizzate. Il "blocco del computer" è l'operazione con cui viene impedito l'accesso alla sessione di lavoro senza chiuderla. L'utilizzo dei dispositivi fisici e la gestione dei dati ivi contenuti devono svolgersi nel rispetto della sicurezza e dell'integrità del patrimonio dati dell'Ente;

2. l'Utente deve quindi eseguire le operazioni seguenti:
    - se si allontana dalla propria postazione, dovrà mettere in protezione il suo dispositivo affinché persone non autorizzate non abbiano accesso ai dati protetti;
    - bloccare il proprio dispositivo prima delle pause e, in generale, ogni qualvolta abbia bisogno di allontanarsi dalla propria postazione;
    - chiudere le sessioni di lavoro (logout) a fine giornata;
    - spegnere il PC dopo il logout dalle suddette sessioni lavorative;
    - controllare sempre che non vi siano persone non autorizzate che possano prendere visione delle schermate del proprio dispositivo.

2.2.4 Corretto utilizzo degli strumenti informatici dell'Ente

L'Utente (ai sensi dell'art. 1.4 del presente manuale) è consapevole che gli strumenti informatici forniti sono di proprietà dell'Ente e devono essere utilizzati esclusivamente per rendere la propria 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 Utente si deve quindi attenere alle seguenti regole di utilizzo degli strumenti informatici.

L'accesso allo strumento informatico (ad es. PC) è protetto da password che deve essere custodita dall'Utente con la massima diligenza e non divulgata. Il dispositivo che viene consegnato all'Utente contiene tutti i software necessari a svolgere le attività affidate dall'Ente.

Per necessità tecniche/operative, gli ADS, utilizzando le proprie credenziali di autenticazione, potranno accedere, per finalità di gestione del sistema e della sua sicurezza e con le regole indicate nel presente Manuale, sia alle memorie di massa locali e di rete (repository e backup) che ai sistemi di elaborazione centrali (server) nonché, accedere ai computer, anche in modalità "da remoto".

In particolare l'Utente deve adottare le seguenti indicazioni:

1. utilizzare solo ed esclusivamente le directory di lavoro appositamente predisposte in rete (ad es. cartelle condivise su file server) ed ivi elaborare i documenti informatici di propria competenza, senza pertanto creare altri file fuori dalle suddette directory di lavoro disponibili sulla rete locale;
2. spegnere il computer, o curarsi di effettuare il logout, prima di lasciare gli uffici o in caso di assenze prolungate, poiché lasciare un elaboratore 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;
3. mantenere sul computer esclusivamente i dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori), consegnati dall'ADS dell'Ente;
4. non dare accesso al proprio computer ad altri Utenti mentre si è loggati con il proprio account a meno di necessità stringenti e sotto il proprio costante controllo;
5. gli strumenti informatici devono essere custoditi con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento e segnalando tempestivamente all'ADS ogni malfunzionamento e/o danneggiamento;
6. è obbligatorio consentire l'installazione degli aggiornamenti di sistema che vengono proposti automaticamente, al primo momento disponibile, in modo tale da mantenere il PC

sempre protetto;
7. Nel caso in cui l'Utente dovesse notare comportamenti anomali del PC, è tenuto a comunicarlo tempestivamente all'ADS.

2.2.5 Divieti espressi sull'utilizzo degli strumenti informatici dell'Ente

L'Utente ha lo specifico divieto di utilizzare gli strumenti informatici concessi in dotazione con le seguenti modalità o per le seguenti attività:

1. gestione, memorizzazione (anche temporanea) o trattamento di file, documenti e/o informazioni personali ad esso riconducibili o comunque non afferenti alle attività lavorative all'interno dell'Ente, nel disco fisso o in altre memorie di massa aziendali e negli strumenti informatici aziendali in genere (es. giochi, files musicali o audiovisivi o immagini, ecc.);
2. modifica delle configurazioni (hardware e software) preimpostate sul personal computer;
3. utilizzo di programmi e/o sistemi di crittografia senza la preventiva autorizzazione scritta da parte dell'ADS;
4. installazione di software di cui l'Ente non possieda la licenza, né installazione alcuna rispetto alle applicazioni o al sistema operativo presenti sul personal computer consegnato, senza l'espressa autorizzazione dell'ADS. È, peraltro, vietato fare copia del software installato al fine di farne un uso personale;
5. installazione o utilizzo di dispositivi hardware "esterni" (ad esempio hard disk, driver, PCMCIA, etc.) e periferiche in genere (telecamere, macchine fotografiche, smartphone, pen drive USB, modem etc.) diversi da quelli consegnati, senza l'autorizzazione espressa dell'ADS;
6. diffusione, intenzionale o per negligenza, di programmi idonei a danneggiare il sistema informatico dell'Ente, quali per esempio virus, trojan horses, ransomware e malware in genere;
7. effettuare in proprio attività manutentive sulla postazione di lavoro;
8. permettere attività manutentive da parte dei soggetti non espressamente autorizzati dell'Ente;
9. divieto di connettere alla rete locale qualsiasi dispositivo (PC esterni, router, switch, modem, stampanti, etc.) non autorizzato preventivamente dall'ADS.

2.2.6 Autorizzazione e profilatura degli Utenti

Le credenziali di autenticazione per l'accesso ai sistemi e alle procedure informatizzate dell'Ente, come già specificato all'art. 2.2.2, vengono assegnate dal RSI ovvero dall'ADS, previa formale richiesta del Responsabile di Settore nell'ambito del quale verrà inserito ed andrà ad operare il nuovo Utente.
Nel caso di collaboratori la preventiva richiesta, se necessaria, verrà inoltrata direttamente dal Responsabile del trattamento con il quale il collaboratore si coordinerà nell'espletamento del proprio incarico. Lo stesso dicasi nel caso di revoca e/o trasferimento.
Gli Utenti, precedentemente autenticati, devono essere autorizzati dal Responsabile di Settore circa l'ambito di accesso/conoscenza del Patrimonio Informativo dell'Ente e le operazioni che su di esso possono eseguire (consultazione, modifica, diffusione, cancellazione etc.).
Sarà cura del Responsabile di Settore in cui opera l'Utente chiedere all'ADS di assegnare e/o modificare i diritti di accesso al sistema informativo dell'Ente, in base alle mansioni assegnate e svolte dall'Utente.
Tutti i dipendenti (o assimilabili come tali ai sensi dell'art. 1.4 del presente manuale) dell'Ente devono, infatti, essere dotati di profili di autorizzazione correlati alle specifiche mansioni.

L’RSI ovvero l’ADS può, anche su indicazione del Settore Personale, automaticamente revocare ogni accesso ai sistemi e alle procedure informatizzate dell’Ente relativi ad Utenti non più in servizio o con cui l’Ente ha terminato il rapporto lavorativo, senza previa comunicazione agli interessati.
La revoca delle credenziali comporta anche la simultanea cancellazione dei dati in esso contenuti, ne consegue che l’Utente prima della cessazione del rapporto di lavoro deve spostare ogni cartella, file, dato, email o informazione necessaria al Settore di appartenenza in una posizione accessibile all’Ente e/o al Responsabile di Settore anche a seguito della cancellazione del proprio account (esempio: cartelle di rete, cartelle condivise, etc). La responsabilità della verifica di tale adempimento è in capo al Responsabile del trattamento con il quale l’utente si è coordinato nell’espletamento del proprio incarico.

2.2.7 Utilizzo infrastruttura di rete e File System

Per l’accesso alle risorse informatiche dell’Ente attraverso la rete locale, ciascun Utente deve essere in possesso di credenziali di autenticazione correlate a specifici profili di autorizzazione secondo gli artt. 2.2.2 e 2.2.6 del presente Manuale.

1. si ribadisce che è assolutamente proibito accedere alla rete ed ai sistemi informativi utilizzando credenziali di altre persone;
2. l’accesso alla rete garantisce all’Utente la disponibilità di condivisioni di rete (cartelle condivise su file server e simili) nelle quali vanno inseriti e salvati i file di lavoro, organizzati per area/ufficio o per diversi criteri o per obiettivi specifici di lavoro. I dispositivi informatici e tutte le cartelle di rete possono ospitare esclusivamente contenuti afferenti l’attività lavorativa. È, pertanto, vietato il salvataggio sui server dell’Ente, ovvero sui dispositivi informatici in genere, di documenti non inerenti l’attività lavorativa, quali a titolo meramente esemplificativo e non esaustivo documenti, fotografie, video, musica, pratiche personali, sms, e-mail personali, film e quant’altro. Ogni materiale personale rilevato dall’ADS a seguito di interventi di gestione della sicurezza informatica ovvero di manutenzione/aggiornamento sui server e sui dispositivi informatici in genere viene rimosso, ferma ogni ulteriore responsabilità civile, penale e disciplinare a carico dell’Utente;
3. tutte le risorse di memorizzazione, diverse da quelle debitamente predisposte per l’archiviazione centralizzata dei dati, quali server e NAS (a titolo esemplificativo e non esaustivo il disco “C” o altri dischi locali dei singoli PC, gli eventuali dispositivi di memorizzazione locali o di disponibilità personale come hard disk portatili o NAS ad uso esclusivo) non sono sottoposte al controllo regolare dell’ADS e non sono oggetto di backup periodici. Tutte queste aree di memorizzazione non devono ospitare dati di interesse, poiché non sono garantite la sicurezza e la protezione contro l’eventuale perdita di dati. Pertanto la responsabilità dei salvataggi dei dati ivi contenuti è a carico del singolo Utente;
4. senza il consenso del Titolare, è vietato trasferire documenti elettronici dai sistemi informativi e dispositivi informatici dell’Ente a device esterni (ad es. hard disk, pen drive USB, CD, DVD e altri supporti);
5. senza il consenso dell’ADS è vietato salvare documenti elettronici dell’Ente su repository esterne (quali ad esempio Dropbox, Whatsapp, Telegram, OneDrive, WeTransfer, etc.), fatto salvo per le piattaforme autorizzate. In caso di necessità l’Ente metterà a disposizione modalità in linea con le presenti direttive;
6. qualora l’Ente mettesse a disposizione dei propri Utenti la possibilità di accedere alle proprie risorse informatiche anche dall’esterno, ciascun Utente è tenuto a seguire tutti gli obblighi del presente Manuale e più in generate ad attuare ogni buona prassi per minimizzare i rischi relativi alle minacce di sicurezza informatica, preservando la disponibilità, integrità e riservatezza dei dati e la continuità dei servizi erogati dall’Ente;

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

2.2.8 Sicurezza della rete

La rete informatica dell’Ente è di fondamentale importanza per il corretto funzionamento di tutte le diverse parti del Sistema Informativo e deve essere pertanto oggetto di particolare attenzione. Ne consegue che devono essere adottate adeguate misure di sicurezza volte a tutelarne il corretto funzionamento.

1. Non è consentita la modifica delle configurazioni impostate di default sul dispositivo;
2. Ogni computer aziendale deve obbligatoriamente essere collegato alla rete aziendale e non può per nessun motivo essere scollegato da tale rete. Casi particolari in cui il computer non debba essere connesso alla rete aziendale devono essere esplicitamente autorizzati dal SIA;
3. I computer portatili devono essere collegati alla rete aziendale con frequenza almeno mensile al fine di garantisce l’aggiornamento di: sistema operativo, antivirus e degli applicativi installati;
4. per ragioni di sicurezza non è concesso connettere alla rete aziendale stazioni di lavoro private e sistemi di connessione (es. modem, switch, hub ecc.) se non su esplicita e formale autorizzazione del SIA;
5. È fatto divieto, per ogni Utente e per ogni Responsabile che autorizzi o affidi a società esterne lavori e/o servizi che per qualsiasi ragione debbano collegarsi alla rete aziendale, di collegare alla rete aziendale qualsiasi oggetto, dispositivo o apparato che non sia stato preventivamente fornito o autorizzato dal SIA.

2.2.9 Gestione delle richieste di accesso al contenuto di risorse ICT

L’Ente, in caso di improvvisa ed indeterminata indisponibilità di un Utente (ad esempio in caso di decesso) potrebbe avere la necessità di recuperare documenti importanti su risorse ICT, assegnate al summenzionato Utente, al fine di proseguire le attività in cui era coinvolto.
In tali casi il Responsabile dell’Area/Servizio di afferenza dell’Utente assegnatario delle risorse ICT potrà chiedere all’ADS di avere accesso alle suddette risorse ICT per estrarre dalle risorse medesime le informazioni indispensabili per proseguire l’attività lavorativa.

2.2.10 Diritti di accesso e controllo remoto

1. Per facilitare le operazioni di aggiornamento del software e per garantire la sicurezza dei dispositivi, delle applicazioni e dei dati, il SIA può avvalersi di strumenti di controllo remoto che consentano di compiere le operazioni necessarie attraverso la rete locale;
2. l’assistenza tecnica per malfunzionamenti ordinari o diagnosi di sistema attraverso strumenti di controllo remoto deve avvenire di norma in presenza dell’utilizzatore stesso;
3. in caso di malfunzionamenti straordinari e in situazioni di emergenza, il SIA ha facoltà in qualunque momento di accedere a qualunque sistema informativo aziendale per l'espletamento delle proprie funzioni.

Il SIA può in qualunque momento procedere alla rimozione di qualsiasi file o applicazione che riterrà essere pericolosa per la sicurezza, sia sulle postazioni degli utenti che sulle unità di rete.

2.3 Soluzioni comportamentali

2.3.1 Uso delle risorse informatiche e fruizione del wifi

Tutti gli Utenti devono utilizzare le risorse ICT, fornite dall'Ente, in maniera diligente, in modo appropriato, efficiente, rispettoso e per motivi lavorativi.
Gli Utenti devono utilizzare le risorse ICT solamente per fini professionali (in relazione alle mansioni assegnate) e per conto dell'Ente, evitando l'uso per attività non pertinenti (ad esempio esecuzione di programmi di intrattenimento, giochi on line, etc.).
Particolare cautela deve essere posta, inoltre, nell'utilizzo di reti wifi gratuite per accedere alla rete Intranet e ai servizi di posta elettronica istituzionale dal momento che nell'accedere a tali servizi devono essere inserite le credenziali e che queste ultime potrebbero essere facilmente carpite da malintenzionati/hacker.
Gli Utenti sono tenuti, inoltre, a:

- sottoporre a scansione antivirus preventiva gli eventuali supporti mobili in dotazione ed espressamente autorizzati (pendrive USB, CDROM/DVD, hard disk esterni, etc.) prima di utilizzare le risorse contenute negli stessi;
- non trasportare le postazioni di lavoro "fisse" al di fuori delle sedi dell'Ente, salvo specifica autorizzazione;
- non accedere alla rete Intranet dell'Ente tramite i propri dispositivi personali.

2.3.2 Utilizzo di dispositivi cellulari, tablet, computer portatili e di archiviazione dati

Fatte salve le regole generali indicate al punto precedente, l'utilizzo di dispositivi cellulari, tablet, computer portatili e di archiviazione dati (pendrive e simili), all'esterno dei locali dell'Ente, deve essere oggetto di particolare cura ed attenzione da parte degli Utenti perché tale utilizzo rappresenta una fonte di rischi particolarmente rilevante in termini di sicurezza, sia delle risorse in sé sia dei dati in esse contenuti.
I dispositivi mobili possono venire concessi in uso dall'Ente agli Utenti che durante gli spostamenti necessitino di disporre di archivi elettronici, supporti di automazione e/o di connessione alla rete dell'Ente.
L'Utente affidatario è responsabile dei dispositivi mobili assegnatigli dall'Ente e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
I dispositivi mobili che permettono l'attivazione di una procedura di protezione con PIN o password devono sempre essere abilitati solo con la digitazione della componente riservata stessa e non possono esserne lasciti privi.
Tali dispositivi, infatti, possono essere soggetti a smarrimento, furti, distruzione o compromissione dei dati, tentativi di frode e/o accesso non autorizzato ovvero essere "infettati" da virus o codice malevolo.
Per altro, un'eventuale contaminazione da virus informatici potrebbe diffondersi e ripercuotersi all'intera rete informatica dell'Ente, una volta che tali dispositivi siano collegati direttamente alla rete interna.
E' necessario, pertanto, adottare ulteriori norme comportamentali nonché specifiche procedure, di seguito descritte, che gli Utenti sono chiamati ad applicare in modo scrupoloso:

- fare periodicamente delle copie di backup dei dati e verificarle regolarmente;
- mantenere abilitato l'antivirus;
- non disabilitare le impostazioni di sicurezza originariamente impostate dall'ADS;
- evitare di accedere e navigare in siti web "pericolosi" per la sicurezza informatica, a prescindere dal fatto che ciò avvenga al di fuori dell'orario di lavoro;

- non mantenere abilitati protocolli insicuri di comunicazione, come ad es. il bluetooth, oltre il tempo strettamente necessario;
- presidiare i dispositivi informatici al fine di evitare l'accesso a soggetti terzi non autorizzati.

2.3.3 Utilizzo di telefoni, scanner, fotocopiatrici 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 all'Utente per rendere la prestazione lavorativa. Pertanto ne viene concesso l'uso esclusivamente per tale fine e con le seguenti modalità:

1. il telefono affidato all'utente 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 all'utente, 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, 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, se consentita.
3. sugli smartphone è vietata l'installazione e l'utilizzo di applicazioni (o altresì denominate "App" nel contesto degli smartphone) diverse da quelle autorizzate dall'ADS.
4. è vietato l'utilizzo dei fax per fini personali, tanto per spedire quanto per ricevere documentazione;
5. è vietato l'utilizzo delle fotocopiatrici e delle stampanti per fini personali;
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;
   - nel caso in cui si rendesse necessaria la stampa di informazioni riservate l'utente dovrà presidiare il dispositivo di stampa per evitare la possibile perdita o divulgazione di tali informazioni a persone terze non autorizzate;

2.3.3.1 Scansione su multifunzione

Scansione da multifunzione con invio a casella di posta elettronica:

1. Le scansioni devono essere inoltrate alla propria mail aziendale per verificarne la corretta scansione. Solo dalla propria casella mail sarà possibile procedere all'inoltro a una persona terza;
2. È proibito l'invio di scansioni da multifunzione verso mail non aziendali.

Scansione da multifunzione con salvataggio su cartella di rete:

1. Qualora il file derivante da scansione venga salvato su una cartella condivisa, l'utente si fa carico di spostare il file in una cartella non consultabile da utenti non autorizzati alla visione del documento;
2. La cartella condivisa nella quale vengono salvate le scansioni viene automaticamente cancellata periodicamente. La cancellazione periodica non dispensa tuttavia l'utente dall'obbligo di cancellare/spostare le scansioni eseguite dalla cartella condivisa nel più breve tempo possibile (al fine di non rendere accidentalmente noto a terzi il contenuto dei

file scansione).
Si raccomanda di porre la massima attenzione nella scansione di documenti contenenti dati personali e sensibili.

2.3.4 Utilizzo di memorie esterne (pendrive usb, hard disk, memory card, cd-rom, dvd, etc.)

Agli Utenti può essere assegnata una memoria esterna (quale una pendrive USB, un hard disk esterno, una memory card, etc.) su cui copiare temporaneamente dei dati per un facile trasporto, o altri usi (es. macchine fotografiche con memory card, etc.).
Questi dispositivi devono essere gestiti con le stesse accortezze di cui all'art. 2.3.2 del presente Manuale e devono essere utilizzati esclusivamente dalle persone a cui sono state affidate e, in nessun caso, devono essere consegnate a terzi.

2.3.5 Modifiche delle risorse ICT

Per quanto riguarda le modifiche si devono distinguere:

a) modifiche hardware dei dispositivi informatici dell'Ente: gli Utenti non devono intervenire sui dispositivi, togliendo, sostituendo o installando componenti hardware (ad esempio masterizzatori CDROM/DVD, schede LAN, etc.) senza eccezione alcuna;
b) modifiche software: gli Utenti non devono modificare i parametri di configurazione dei dispositivi assegnati, salvo che ciò avvenga su precisa autorizzazione dell'ADS. Sono fatte salve le personalizzazioni a livello Utente che non abbiano conseguenze impattanti sulla funzionalità dei dispositivi stessi.

Gli Utenti, inoltre, non devono alterare la configurazione originaria del dispositivo ricevuto in uso (ad es. disinstallando, eseguendo o installando applicazioni che interferiscano sul funzionamento del dispositivo medesimo) senza autorizzazione dell'ADS.

2.3.6 Smarrimento e furto delle risorse ICT

Nei casi di smarrimento, furto accertato o grave manomissione dei dispositivi assegnati o del loro contenuto, gli Utenti devono segnalare tempestivamente l'accaduto ai soggetti di seguito indicati:
a) Autorità Giudiziaria (sporgendo denuncia);
b) Titolare e Responsabile del trattamento dei dati;
c) RSI e ADS dell'Ente;

2.3.7 Distruzione dei dispositivi

Ogni dispositivo ed ogni memoria esterna affidati agli Utenti, (computer, notebook, tablet, smartphone, memory card, chiavi usb, hard disk, dvd, cd-rom, etc.), al termine del loro utilizzo dovranno essere restituiti all'Ente, che provvederà a distruggerli o a ricondizionarli seguendo le norme di legge in vigore al momento.
In particolare, l'Ente provvederà a cancellare o a rendere inintelligibili i dati negli stessi memorizzati.

3 Gestione dei dati

Il patrimonio informativo e di conoscenza detenuto dall'Ente e di cui esso è Titolare si suddivide in due macroaree:

- dati personali;
- dati (riservati o non riservati) diversi da quelli personali.

Le due fattispecie necessitano di trattamenti peculiari, fatte salve le più generali cautele e misure di sicurezza descritte a proposito dei dispositivi come più sopra indicato.

3.1 I dati personali

In questa sezione del Manuale si vuole porre l'attenzione sugli aspetti di sicurezza relativi al trattamento di dati personali.
Ai fini della corretta applicazione delle indicazioni che seguono, si ritiene utile riportare di seguito la classificazione dei dati personali fatta dal legislatore.
Ai sensi dell'art. 4 del GDPR, è un "dato personale", qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
I dati personali devono essere:

a) trattati e protetti secondo quanto previsto dal GDPR e dal D. Lgs. 196/03 e ssmmii;
b) custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
c) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici;
d) trattati in maniera da garantire un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»);
e) distrutti o resi inutilizzabili all'atto della dismissione di supporti che li contengano (cancellandone il contenuto), secondo quanto previsto dal Provvedimento del Garante per la protezione dei dati personali del 13 ottobre 2008 sui "Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali".

3.1.1 Dati particolari/sensibili e giudiziari/ relativi a condanne penali e reati

Tutti gli Utenti devono porre particolare attenzione nei trattamenti di categorie particolari di dati personali (definiti all'art. 9 del GDPR ed all'art. 4 del Codice) in relazione alla confidenzialità dei dati.
Sono indicati alcuni comportamenti o regole minime da rispettare: cifrare i dati memorizzati sui

file/database o in fase di trasferimento; proteggere i canali di trasmissione; evitare l'invio con la posta elettronica di dati sensibili e giudiziari; recuperare tempestivamente i documenti stampati o ricevuti via fax che contengano dati sensibili o giudiziari per sottrarli alla vista di chi non è autorizzato; separare logicamente i dati "comuni" da quelli sensibili/giudiziari nei database, etc.

3.2 I dati diversi da quelli personali

Fatto salvo il requisito dell'Integrità, i dati diversi da quelli personali (definiti al precedente art. 3.1 del presente Manuale) sono classificati in base al livello di Confidenzialità (Confidentiality) come segue:

1. dati riservati;
2. dati non riservati.

3.2.1 Dati riservati

Appartengono a questa categoria i dati a cui siano collegati interessi giuridicamente rilevanti (come ad es. la proprietà individuale, il diritto d'autore e i segreti commerciali).
La gestione, trasmissione e condivisione dei dati riservati deve essere sottoposta a particolari cautele e misure, stabilite dal soggetto responsabile, al fine di preservare la confidenzialità dei dati medesimi.
L'eventuale manutenzione, effettuata da partner privati, sui sistemi ed apparati che ospitano dati riservati deve essere disciplinata, a livello contrattuale, prevedendo specifici obblighi di riservatezza a carico dei partner privati.

3.2.2 Dati non riservati

Appartengono a questa categoria: i dati il cui accesso e/o utilizzo non ha restrizioni (ad es. gli "Open Data", i dati oggetto di "accesso civico", etc.)
Per i dati non riservati, il Titolare stabilisce le forme e modalità attraverso cui rendere disponibili e/o liberamente accessibili i dati nel rispetto della normativa vigente.

4 Modalità e doveri nell'utilizzo di posta elettronica, internet, social media e cloud computing

4.1 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 Utente si deve attenere alle seguenti regole di utilizzo dell'indirizzo di posta elettronica:

1. Gli Utenti cui viene fornito un account e-mail nominativo, generalmente coerente con il modello nome.cognome@dominio dell'Ente, sono tenuti ad utilizzare la e-mail esclusivamente a scopi lavorativi: è assolutamente vietato ogni utilizzo di tipo privato. L'utente 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, ufficio o gruppo 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 la sicurezza della rete, 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 eseguibile, ad esempio, *.exe, *.com, *.vbs, *.htm, *.scr, *.bat, *.js , *.pif, *.cab, *.zip, *.rar, ovvero collegamenti (link) a siti esterni. 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 l'ADS 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" (oltre a 10MB) 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 verificare insieme all'ADS altri strumenti più idonei allo scopo;
7. nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati personali o dati sensibili, è obbligatorio che questi allegati vengano preventivamente resi inintelligibili attraverso crittazione con apposito software (archiviazione e compressione con password). La password di cifratura deve essere comunicata al destinatario attraverso un canale diverso dalla e-mail (ad esempio 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 di "Assenza dall'Ufficio", tramite risponditore automatico, facendo menzione di chi, all'interno dell'Ente, assumerà le mansioni durante l'assenza;
9. in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, qualora non fosse possibile attivare la funzione di risponditore automatico 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 Responsabile del Servizio quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Sarà compito del Responsabile del Servizio 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, possibilmente su autorizzazione del Responsabile di Servizio 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 Utente, 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 directory disponibili su file server.

4.2 Navigazione in 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 Utente 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, ad es. i siti istituzionali, i siti degli Enti locali, di fornitori e partner. L'accesso può essere regolato dal proxy con le sue policy di sicurezza debitamente implementate e aggiornate;
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 dall'ADS;
4. l'Ente si riserva di bloccare l'accesso a siti "a rischio" attraverso l'utilizzo di blacklist 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, l'Utente potrà contattare l'ADS per uno sblocco selettivo;
5. è vietato accedere ad alcuni siti internet mediante azioni inibenti dei filtri, sabotando o comunque superando o tentando di superare o disabilitando i sistemi adottati dall'Ente per bloccare accessi non conformi all'attività lavorativa. In ogni caso è vietato utilizzare siti o altri strumenti che realizzino tale fine;
6. nel caso in cui, per ragioni di servizio, si necessiti di una navigazione più libera da filtri, è necessario che il Responsabile di Settore di afferenza dell'utente richieda lo sblocco mediante una e-mail indirizzata all'ADS (helpdesk@unionerubiconemare.it), nella quale siano indicati chiaramente: motivo della richiesta, utente e postazione da cui effettuare la navigazione libera, intervallo di tempo richiesto per completare l'attività;
7. è assolutamente vietato l'utilizzo di abbonamenti privati per effettuare la connessione a Internet;
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 nickname);
9. è consentito l'uso di strumenti di messaggistica istantanea, per permettere una efficace e comoda comunicazione tra i colleghi, mediante i soli strumenti autorizzati dall'ADS. Tali strumenti hanno lo scopo di migliorare la collaborazione tra utenti aggiungendo un ulteriore canale comunicativo rispetto agli spostamenti fisici, alle chiamate telefoniche ed alle e-mail. È consentito un utilizzo legato esclusivamente a scopi professionali;

4.3 Utilizzo dei social media

L'utilizzo e la consultazione di social media sono permessi esclusivamente per finalità istituzionali, attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli Utenti.

Il dipendente è responsabile del corretto uso delle risorse informatiche, con particolare riferimento

ai dati trattati a fini istituzionali. È, altresì, responsabile del contenuto delle comunicazioni social 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. Sono vietati comportamenti che possano creare un danno, anche di immagine, all'Amministrazione.
Durante l'orario di lavoro e con i dispositivi forniti dall'ente è vietato l'utilizzo di social network (Facebook, Twitter, ecc) a tutti i dipendenti, salvo i casi autorizzati dal Dirigente/Responsabile.
Il dipendente nell'utilizzo, anche privato, dei social network si astiene dal pubblicare dichiarazioni offensive nei confronti dell'Amministrazione, giudizi sull'operato dell'Amministrazione derivanti da informazioni assunte nell'esercizio delle proprie funzioni che possano anche recare danno all'Amministrazione stessa, nonché dichiarazioni offensive, discriminatorie o di scherno nei confronti dei colleghi e dei superiori. Si astiene altresì dal pubblicare foto, video e audio lesive dell'immagine dell'Amministrazione, dell'onorabilità, della riservatezza e della dignità dei colleghi e degli amministratori;
Il dipendente osserva anche sui social network il segreto d'ufficio e la normativa in materia di tutela e trattamento dei dati personali come previsto dal comma 5, art. 12 del DPR n.62 del 2013. È severamente vietato divulgare informazioni riservate e interne, nello specifico: corrispondenza interna, informazioni di terze parti (ad esempio relative a partner, istituzioni, utenti, stakeholder, etc.) o informazioni su attività lavorative di cui si è a conoscenza per ragioni d'ufficio.

4.4 Utilizzo di sistemi cloud computing

In informatica con il termine inglese cloud computing (in italiano nuvola informatica) si indica un paradigma di erogazione di risorse informatiche, come l'archiviazione, l'elaborazione o la trasmissione di dati, caratterizzato dalla disponibilità on demand attraverso Internet a partire da un insieme di risorse preesistenti e configurabili.
Utilizzare un servizio di cloud computing per memorizzare dati personali, espone l'Ente a potenziali problemi di violazione della privacy. I dati personali vengono memorizzati nelle server farms di aziende che spesso risiedono in uno stato diverso da quello dell'Ente. Il cloud provider, in caso di comportamento scorretto o malevolo, potrebbe accedere ai dati personali per eseguire ricerche di mercato e profilazione degli utenti. In presenza di atti illegali, come appropriazione indebita o illegale di dati personali, il danno potrebbe essere molto grave per l'Ente, con difficoltà di raggiungere soluzioni giuridiche e/o rimborsi se il fornitore risiede in uno stato diverso dal paese dell'utente.
Per quanto indicato gli Utenti dovranno rispettare le seguenti indicazioni:

1. è vietato agli Utenti l'utilizzo di sistemi cloud non espressamente approvati dall'Ente. Per essere approvati, i sistemi cloud devono rispondere ad almeno i seguenti requisiti:
   - essere sistemi cloud esclusivi e non condivisi;
   - essere sistemi cloud posizionati fisicamente nell'Unione Europea.
2. l'azienda che fornisce il sistema in cloud deve essere preventivamente nominata Responsabile del Trattamento dei dati da parte dell'Ente;
3. l'azienda che fornisce il sistema in cloud deve comunicare all'Ente, almeno una volta all'anno, i nominativi degli amministratori di sistema utilizzati;
4. dovranno essere verificate tutte le indicazioni e prescrizioni previste dal Garante della Privacy nei suoi provvedimenti sugli Amministratori di Sistema e sul cloud;
5. I soli sistemi in Cloud autorizzati per gli Enti pubblici sono quelli qualificati Agid;

5 Protezione Antivirus

I virus (o più in generale qualsiasi software malevolo) possono essere trasmessi tramite scambio di file via internet, via e-mail, scambio di supporti removibili, file-sharing, chat, etc.
L'Ente impone su tutte le postazioni di lavoro (fisse e mobili) l'utilizzo di un sistema Antivirus correttamente installato, attivato e continuamente aggiornato automaticamente con frequenza almeno quotidiana.
L'Utente, da parte sua, deve impegnarsi a controllare il corretto funzionamento e aggiornamento del sistema Antivirus installato sul proprio computer e, in particolare, deve rispettare le regole seguenti:

1. comunicare all'ADS ogni anomalia o malfunzionamento del sistema antivirus;
2. comunicare all'ADS eventuali segnalazioni di presenza di virus o file sospetti.

Inoltre, all'Utente:

1. è vietato accedere alla rete aziendale senza servizio antivirus attivo e aggiornato sulla propria postazione;
2. è vietato ostacolare l'azione dell'antivirus aziendale;
3. è vietato disattivare l'antivirus senza l'autorizzazione espressa dell'ADS, anche e soprattutto nel caso sia richiesto per l'installazione di software sul computer.

6 Controlli

L'Ente, in qualità di Titolare dei dati trattati dagli Utenti nonché Titolare degli strumenti informatici e dei dati ivi contenuti e/o trattati, si riserva la facoltà di effettuare i controlli che ritiene opportuni per le seguenti finalità:

- tutelare la sicurezza e preservare l'integrità degli strumenti informatici e dei dati;
- evitare la commissione di illeciti o per esigenze di carattere difensivo anche preventivo;
- verificare la funzionalità del sistema e degli strumenti informatici.

Le attività di controllo potranno avvenire anche con audit e vulnerability assesment del sistema informatico. Per tali controlli l'Ente si riserva di avvalersi di soggetti esterni.
Si precisa, in ogni caso, che l'Ente non adotta "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori" (ex art. 4, primo comma, l. n. 300/1970), tra cui sono certamente comprese le strumentazioni hardware e software mirate al controllo dell'Utente.
In applicazione del principio di necessità di cui all'art. 3 del D. Lgs 196/03 e ssmmii, l'Ente promuove ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri e, comunque, a "minimizzare" l'uso di dati riferibili agli Utenti e allo scopo ha adottato idonei strumenti, organizzativi e fisici, volti a prevenire trattamenti illeciti sui dati trattati con strumenti informatici.
L'Ente informa di non adottare sistemi che determinano interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.
In particolare, eventuali sistemi atti a monitorare eventuali violazioni di legge o comportamenti anomali da parte degli Utenti avvengono nel rispetto del principio di pertinenza e non eccedenza, con esclusione di registrazioni o verifiche con modalità sistematiche.

7 Violazioni

L'eventuale violazione delle norme e/o delle buone regole di comportamento può comportare l'applicazione in capo ai contravventori di sanzioni di tipo civile, penale e/o disciplinare.

8 Entrata in vigore, pubblicità e aggiornamento

Le regole contenute nel presente Manuale entrano in vigore dalla data di adozione del provvedimento di approvazione.
Del presente Manuale sarà fornita massima pubblicità mediante la diffusione sull'intranet dell'Ente.
Il presente Manuale sarà oggetto di aggiornamento ogni volta che se ne ravvisi la necessità, in caso di variazioni tecniche dei sistemi dell'Ente o in caso di mutazioni legislative. Ogni variazione del presente Manuale sarà prontamente comunicata agli Utenti.