Allegato A

Approvato con Delibera di Giunta n.299 del 17.11.2021

Comune di Alghero
Provincia di Sassari

Il Titolare del Trattamento	Dott. Alessandro Alciator
Il DPO	Dott. Danilo Cannas
Il Responsabile Transizione al Digitale	Dott. Alessandro Alciator
L'Amministratore di Sistema	Dott. Alessandro Alciator

MANUALE INTERNO PER L'UTILIZZO DELLE RISORSE ICT 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.

REV_00 del _10/11/2021

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 dispostivi informatici, espongono l'Ente e gli Utenti (come definiti all'**art. 1.4**) a rischi di natura patrimoniale, oltre alle 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, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, e che tutte le risorse ICT (Information and Communication Technology), fornite dall'Amministrazione agli Utenti devono essere utilizzate in modo appropriato, efficiente, rispettoso e 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*, tablets,* 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, pendrive, etc.*);
- i sistemi e i canali di comunicazione (tipo *e-mail*, PEC, connessione ad *internet* e simili);
- i dispositivi di stampa;
- i dispositivi per l'elaborazione e l'archiviazione centralizzata dei dati (tipo *server, NAS* e simili);
- 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) nr. 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) Enti e Agenzie attestati alla rete Intranet dell'Ente, per quanto applicabile.

Le prescrizioni tecnico/organizzative si rivolgono a differenti categorie di soggetti 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.).

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.

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 comunale.

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 non ricoprente 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.
Per gli incidenti che possono determinare una violazione dei dati personali, cioè la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (cd. "*databreach*") l'art. 33 del GDPR prevede che in caso di violazione dei dati personali, "*il titolare del trattamento notifica la violazione all'autorità di controllo senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo*".
Il successivo art. 34 disciplina il caso in cui la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche: in tal caso è necessario comunicare la violazione all'interessato senza ingiustificato ritardo, a meno che non si verifichino le circostanze indicate nel paragrafo 3 dell'articolo:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati.

Per ottemperare agli obblighi imposti dalla norma, ogni Utente avvisa senza indugio il Responsabile del trattamento dei dati, segnalando le violazioni o gli incidenti informatici che ha rilevato e che possono avere un impatto significativo sui dati personali. Il Responsabile del trattamento dei dati, ricevuta la notizia dell'avvenuto incidente di databreach, avvisa senza indugio il Titolare, il RSI e l'ADS. Ricevuta l'informazione di avvenuto databreach, il Titolare del trattamento procede, ai sensi dell'art. 33, paragrafo 1, GDPR 679/2016, notificando la violazione all'autorità di controllo senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

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 assimilati tali) dell'Ente devono infatti essere dotati di credenziali di autenticazione al sistema informatico.

Gli Utenti devono essere identificati e ricevere dall'ADS, previa formale richiesta del Responsabile di Area/Servizio nell'ambito del quale verrà inserito ed andrà ad operare il nuovo Utente, 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 sono disabilitate dall'ADS, 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 14 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) 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 per alcuni minuti.
9) Le regole su elencate sono da considerarsi un punto di partenza, ma non vanno intese come prinicpi cristallizzati nel tempo, valevoli per sermpre, 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 (dipendente o assimilato tale) è consapevole che gli strumenti informatici 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 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, previa comunicazione al dipendente, accedere al *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), disposti dall'ADS dell'Ente;
4) non dare accesso al proprio *computer* ad altri Utenti, a meno che non siano quelli con cui è condiviso l'utilizzo dello stesso PC o 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 datigli 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;
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) archiviazione, anche temporanea, sul disco fisso del *computer* o nel *file server* di documenti, giochi, *files* musicali o audiovisivi o immagini diversi da quelli necessari allo svolgimento delle mansioni affidate;
6) 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;
7) 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;
8) effettuare in proprio attività manutentive sulla postazione di lavoro;
9) permettere attività manutentive da parte dei soggetti non espressamente autorizzati dell'Ente;
10) 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 Area/Servizio 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 coordina 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 Area/Servizio 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 Area/Servizio in cui opera l'Utente chiedere al Responsabile del trattamento 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 assimilati tali) dell'Ente devono infatti essere dotati di profili di autorizzazione correlati alle specifiche mansioni.

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 *files* 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. Pertanto è vietato il salvataggio sui *server* dell'Ente, ovvero sui dispositivi informatici in genere, di documenti non inerenti l'attività lavorativa, quali a titolo esemplificativo 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*, non sono sottoposte al controllo regolare dell'ADS e non sono oggetto di backup periodici. A titolo esemplificativo e non esaustivo si citano: il disco "C" o altri dischi locali dei singoli PC, la cartella "Documenti" o "*Desktop*" dell'Utente, gli eventuali dispositivi di memorizzazione locali o di disponibilità personale come *hard disk* portatili o *NAS* ad uso esclusivo. 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 (ad esempio pervenuti via *e-mail* o salvati su *server* o sul dispositivo informatico in dotazione) su *repository* esterne (quali ad esempio *Dropbox, Google Drive, OneDrive, WeTransfer*, etc.) ovvero inviarli a terzi via posta elettronica o con altri sistemi. 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, tale accesso dovrà avvenire esclusivamente mediante rete *VPN* (*Virtual Private Network*), un canale privato e criptato verso la rete interna o altre modalità congrue allo stesso scopo;
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 concreta minaccia per la sicurezza informatica.

2.2.8 Sicurezza dei sistemi di elaborazione e archiviazione dati centralizzati

Il sistema informativo di un Ente rappresenta un punto cardine nell'attività lavorativa dell'Amministrazione per l'erogazione dei servizi a cittadini e imprese. Il sistema informativo è a sua volta basato su un sistema informatico che, in caso di anomalie di funzionamento, potrebbe causare l'interruzione di molteplici servizi, provocando disservizio agli utenti e di conseguenza ai dipendenti dell'Amministrazione.

Il Centro Elaborazione Dati (CED) di un Ente deve essere considerato come infrastruttura critica tale per cui il suo corretto funzionamento rappresenta il requisito indispensabile per la regolare erogazione dei servizi.
Il sistema informatico racchiude infatti gran parte del patrimonio di dati e informazioni di cui l'Ente è titolare, visto l'utilizzo massiccio e quasi esclusivo delle tecnologie ICT nell'attività lavorativa dell'Amministrazione. Pertanto, una minaccia alla sicurezza del sistema informatico rappresenta una potenziale indisponibilità dei dati e delle informazioni in esso custoditi e dei servizi che tramite esso sono erogati.
Risulta pertanto indispensabile provvedere ad una adeguata gestione, nonché alla sicurezza, sia fisica che logica, dei sistemi informatici che costituiscono l'infrastruttura del CED dell'Ente.
A questo proposito è indispensabile configurare i sistemi di elaborazione e archiviazione dati centralizzati (*server, NAS*, e simili), nonché i dispositivi individuali, conformemente agli standard di sicurezza e/o *best practices* (ad es. abilitare soltanto i servizi strettamente necessari, applicare sistematicamente le "*pacth*", etc.) emessi da Enti ed Organizzazioni internazionali (ad es. *International Standard Organization* - ISO, *National Institute of Standards and Technology* - NIST, *Sans Intitute*, etc.).
Laddove l'Ente si avvalga di propri fornitori dovrà prevedere nei contratti di appalto l'obbligo di rispettare i predetti standard di sicurezza e, inoltre, dovrà prevedere clausole di "responsabilità esterna" e di "amministrazione dei sistemi", in attuazione del Provvedimento Generale del Garante dei dati personali del 27.11.2008 (in materia di Amministratori di Sistema), come modificato con successivo Provvedimento Generale del 25.06.2009.

2.2.9 Sicurezza delle applicazioni

Gli Enti che sviluppino applicazioni informatiche devono rispettare l'approccio della "*privacy by design*", incorporando sia i principi e le misure a tutela della privacy nell'intero ciclo di vita delle applicazioni che, per le applicazioni *web based*, le *best practices* emesse dall'Organizzazione internazionale *Open Web Application Security Project (OWASP)*.
Il GDPR, al 78° "considerando" iniziale stabilisce che: " *in fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati. I principi della protezione dei dati fin dalla progettazione e di default dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici*."
Gli Enti, qualora affidino ad un fornitore l'incarico di sviluppare applicazioni devono, pertanto, prevedere nei relativi contratti di appalto il rispetto delle stesse prescrizioni di cui al precedente punto.

2.2.10 Sicurezza della rete

L'Amministratore di Rete, (qualora non coincida con L'ADS) configura la Rete Telematica dell'Ente per contribuire alla protezione dei sistemi informatici con strumenti e livelli di protezione (ad es. *firewall, IPS, application firewall*, etc.) adeguati in base al livello di classificazione assegnato ai dati ospitati nei suddetti sistemi (*server, NAS*, e simili).

2.2.11 Gestione della disponibilità (salvataggio e ripristino dei dati)

L'Ente che ha presso le proprie sedi Istituzionali sistemi di elaborazione e archiviazione dati centralizzati (*server, NAS*, e simili) gestiti in proprio deve prevedere idonee politiche di "*backup*" e "*restore*" dei dati in modo da garantire la disponibilità degli stessi, mitigando l'impatto causato da eventuali incidenti e/o errori che dovessero verificarsi nella gestione dei dati.
Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.

2.2.12 Gestione dei log file

Gli Enti che hanno presso le proprie sedi Istituzionali sistemi di elaborazione e archiviazione dati centralizzati (*server, NAS*, e simili) gestiti in proprio devono attivare un sistema di raccolta delle informazioni relative all'accesso ai dati, sistemi, reti ed applicazioni utilizzati dall'Organizzazione, in attuazione del Provvedimento Generale del Garante dei dati personali del 27.11.2008 (in materia di Amministratori di Sistema) come modificato con successivo Provvedimento Generale del 25.06.2009.

2.2.13 Gestione delle richieste di accesso al contenuto di risorse ICT

L'Ente in caso di Utenti deceduti, sospesi o cessati dal servizio, potrebbe avere la necessità di recuperare documenti importanti su risorse ICT, assegnate ai predetti Utenti, al fine di proseguire le attività in cui gli Utenti medesimi erano coinvolti.
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.

2.3 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.).
Al fine di scongiurare i rischi derivanti dall'effetto "*bridge*" (ponte) tra la rete *Intranet* aziendale ed altre reti, gli Utenti devono evitare di accedere dall'esterno della rete *Intranet* ai servizi di posta elettronica istituzionali e/o al servizio *web* dell'Ente e contemporaneamente ad altri siti *Internet* potenzialmente pericolosi.
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 negli stessi contenuti;
- non trasportare le postazioni di lavoro "fisse" al di fuori delle sedi dell'Ente, salvo specifica autorizzazione;
- non accedere alle caselle di posta elettronica istituzionale tramite i propri dispositivi personali;
- 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 nelle stesse 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 abilitabili 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:

- cifrare i dati (laddove possibile e previa analisi dei rischi/costi-benefici);
- 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, ovvero utilizzare la funzione di "stampa protetta".

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 od 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;
d) *Provider* di servizi di telecomunicazione (telefonia e *internet*).

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 dei dati personali particolari/sensibili e giudiziari relativi a condanne penali e reati (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**) 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 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) ad ogni Utente viene fornito un *account e-mail* nominativo, generalmente coerente con il modello *nome.cognome@dominio dell'Ente*. L'utilizzo della *e-mail* deve essere limitato esclusivamente a scopi lavorativi, ed 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" (fino 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 rivolgersi all'ADS;
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 "*Out of Office*" facendo menzione di chi, all'interno dell'Ente, assumerà le mansioni durante l'assenza, oppure indicando un indirizzo *e-mail* alternativo preferibilmente di tipo collettivo, tipo *ufficio….@ dominio Ente*. Rivolgersi all'ADS 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 *auto-reply* 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 Ransomware

Il *ransomware* è un software "malevolo" in grado di "infettare" un dispositivo digitale (PC, tablet, smartphone, smart TV), prendendolo "in ostaggio", ovvero bloccando l'accesso a tutti o ad alcuni dei suoi contenuti (foto, video, file, etc.) al fine di richiedere il pagamento di un riscatto da versare per riottenere l'accesso ai file criptati. La richiesta di pagamento e relative istruzioni, viene visualizzata sullo schermo del dispositivo infettato, in una finestra ad apertura automatica. All'utente viene comunicato il tempo dispobile per il pagamento del riscatto, (solitamente poche ore o giorni), in caso contrario, il blocco dei contenuti diventerà definitivo. Spesso la somma richiesta, cresce con il passare del tempo.

La grande varietà di *ransomware*, in circolazione, può essere ricondotta a due categorie principali:

- i *cryptor* (che criptano i file contenuti nel dispositivo rendendoli inaccessibili);
- i *blocker* (che bloccano l'accesso al dispositivo infettato).

Il *ransomware* si diffonde soprattutto attraverso comunicazioni ricevute via e-mail, sms o sistemi di messaggistica, molto più raramente tramite forme di attacco informatico (attività di controllo e comando) da remoto, che vanno a buon fine sfruttando le falle di vulnerabilità presenti nel sistema attaccato.

Le modalità d'infezione più frequenti, vedono sempre la partecipazione attiva dell'utente bersaglio che, inconsapevolmente, provoca l'ingresso del malware sul proprio dispositivo attraverso comunicazioni che:

- sembrano apparentemente provenire da soggetti conosciuti e affidabili (corrieri espressi, gestori di servizi, operatori telefonici, pubbliche amministrazioni) oppure da persone fidate (colleghi di lavoro, conoscenti);
- contengono allegati da aprire (spesso "con urgenza"), oppure *link* e *banner* da cliccare (per verificare informazioni o ricevere importanti avvisi) collegati a software malevoli;
- possono essere scaricati sul dispositivo quando l'utente clicca *link* o *banner* pubblicitari su siti web (un canale molto usato è rappresentato dai siti per adulti) o social network o naviga su siti web creati ad hoc o "compromessi" da *hacker* per diventare veicolo del contagio *ransomware*;
- possono essere installati attraverso software e app (giochi, utility, addirittura falsi anti-virus) offerti gratuitamente per invogliare gli utenti al download e finiscono così per infettare i loro dispositivi.

Per di più, ogni dispositivo "infettato" ne può "contagiare" altri. Il *ransomware* può diffondersi sfruttando, ad esempio, le sincronizzazioni tra dispositivi, i sistemi di condivisione in cloud e può utilizzare la rubrica dei contatti per spedire automaticamente ad altre persone messaggi contenenti *link* e allegati che diventano veicolo del *ransomware*.

La più importante forma di difesa per evitare l'infezione da *ransomware* è la prudenza. Anche se i messaggi provengono da soggetti a noi noti, **non bisogna mai**:

1) aprire allegati di cui si ignora il contenuto;
2) cliccare su link o banner sospetti;
3) aprire allegati con estensioni non convenzionali (vedi quanto specificato al n° "4)" del precedente punto "*4.1 posta elettronica*");
4) scaricare software da siti sospetti (che per esempio, offrono gratuitamente prodotti commerciali solitamente a pagamento); app e programmi andrebbero scaricati esclusivamente da market ufficiali, i cui gestori effettuano controlli sui prodotti;
5) aprire messaggi apparentemente inviati ad utenze (telefoniche, di fornitura energia, etc.) di cui non si è cliente o da un corriere espresso da cui non si aspettano consegne, e così via;
6) e, naturalmente, aprire messaggi provenienti da soggetti sconosciuti o con i quali non si hanno rapporti.

Oltre alla prudenza, è bene adottare sempre alcuni utili accorgimenti, quali:

1) controllare, senza aprire, l'indirizzo *URL* reale di eventuali *link* o *banner* pubblicitari ricevuti via e-mail o presenti su siti web, così da poter verificare se il *link* da aprire corrisponde al link che appare nel testo del messaggio;
2) mantenere costantemente aggiornati il sistema operativo oltre che il parco software e le app installate;
3) Installare su tutti i dispositivi un antivirus con estensioni anti-*ransomware*.

L'unica vera garanzia però, che ci tutela dal *ransomware* è adottare una politica di *disaster recovery* e continuità operativa (e testarla) che permetta di avere sempre disponibilie una copia di backup aggiornata che, in caso di necessità, permetta di ripristinare i dati contenuti nei dispositivi infettati e di rimettere in linea i sistemi in un tempo ragionevole, in ossequio al rispetto dei prinicipi di disponibilità, confidenzialità ed integrità dei dati.

Il pagamento del riscatto invece è una soluzione che non dovrebbe mai essere presa in considerazione. Oltre al danno economico, si corre il rischio di non ricevere i codici di sblocco, di finire in "liste di pagatori" potenzialmente soggetti a periodici attacchi *ransomware*.

Qualora non si sia in grado di ripristinare i contenuti bloccati, come su esposto, ci si può rivolgere a tecnici qualificati, specializzati, in grado di tentare di sbloccare il dispositivo.

L'ipotesi residuale, qualora l'importanza dei dati bloccati lo consenta, è la formattazione della memoria di massa del dispositivo che, ovviamente, oltre ad eliminare il *malware*, comporta la perdita di tutti i dati in esso contenuti.

Si raccomanda infine, di denunciare sempre l'attacco *ransomware* eventualmente subito alla Polizia Postale (https://www.commissariatodips.it) anche nell'intento di aiutare a prevenire l'ulterioriore diffusione.

4.3 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 libera dai filtri, è necessario richiedere lo sblocco mediante una *e-mail* indirizzata all'ADS, 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. Al termine dell'attività l'ADS ripristinerà i filtri alla situazione iniziale;
7) 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 dall'ADS, con il rispetto delle normali procedure di acquisto;
8) è assolutamente vietato l'utilizzo di abbonamenti privati per effettuare la connessione a *Internet* tranne in casi del tutto eccezionali e previa autorizzazione dell'ADS;
9) 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*);
10) 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;
11) l'utilizzo e la consultazione di *social network* 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;
12) 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 *youtube*, siti di informazione, siti di *streaming* ecc.) o *web radio*, in quanto possono limitare e/o compromettere l'uso della rete agli altri Utenti.

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.

Le risorse non vengono pienamente configurate e messe in opera dal fornitore apposta per l'utente, ma gli sono assegnate, rapidamente e convenientemente, grazie a procedure automatizzate, a partire da un insieme di risorse condivise con altri utenti lasciando all'utente parte dell'onere della configurazione. Quando l'utente rilascia la risorsa, essa viene similmente riconfigurata nello stato iniziale e rimessa a disposizione nel *pool* condiviso delle risorse, con altrettanta velocità ed economia per il fornitore.

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. Con i collegamenti *wireless* "liberi", il rischio sicurezza aumenta e si è maggiormente esposti ai casi di pirateria informatica a causa della minore sicurezza offerta dalle reti senza fili ad accesso libero. 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. 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.
A tale scopo, l'Ente redigerà l'elenco dei soggetti autorizzati ad effettuare operazioni tecniche e di controllo sugli strumenti e dispositivi IT, messi a disposizione dall'Ente, in uso agli Utenti, che possano impattare sul controllo del loro operato a seguito dell'attività di tali soggetti. L'elenco sarà corredato da apposita scheda dei privilegi ad essi attribuiti e conterrà l'indicazione della tipologia, periodicità e tempistiche dei controlli, costantemente monitorati dalla generazione di report dei log di accesso relativi alle attività di controllo effettuate dai soggetti incaricati.
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.
Qualora nell'ambito di tali verifiche si dovesse rilevare un evento dannoso, una situazione di pericolo o qualche altra modalità non conforme all'attività lavorativa (es. scarico di file pirata, navigazioni da cui sia derivato il download di virus informatici, etc.) si effettuerà un avvertimento in modo generalizzato con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.
L'Ente rende

7. CONSERVAZIONE

I sistemi informatici sono stati programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad *Internet* e al traffico telematico, la cui conservazione non sia necessaria.

Un eventuale prolungamento dei tempi di conservazione viene valutato come eccezionale e deve aver luogo solo in relazione:

- ad esigenze tecniche o di sicurezza del tutto particolari;
- all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'Autorità Giudiziaria o della Polizia Giudiziaria.

In questi casi, il trattamento dei dati personali è limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

8. 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.

9. 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.