REGOLAMENTO PER LA GESTIONE E L'UTILIZZO DEI SISTEMI INFORMATICI E TELEMATICI COMUNALI

Data rilascio definitivo del documento: 09/07/2026	Data prima approvazione:	Data ultima modifica: [Vedi tabella di controllo versioni]	Data prossima Review:
Prima approvazione da parte di:	Area 4 Sistemi Informatici Giunta Comunale		
Autori:	dott. Davide Cecchini dott.ssa Michela Castelli Sig. Nico Mariani Sig.ra Spadini Daniela DPO dott. Emanuele Cofanelli Francesco Moroncini– Morolabs Srl		
Responsabile della UO:			
Documenti di supporto, Procedure e modulistica:	Amministrazione Trasparente -> Riferimenti normativi su organizzazione e attività		
Legislazione rilevante in materia:	Riportata in appendice		
Audience:	Dipendenti e fornitori		

Il presente Regolamento deve necessariamente adattarsi alla continua evoluzione normativa, alle nuove tecnologie e ai nuovi dispositivi che potranno essere introdotti in futuro nell'organizzazione; per questo motivo i lettori sono invitati a segnalare eventuali inesattezze, modifiche o integrazioni che si rendessero necessarie utilizzando l'indirizzo e-mail di seguito riportato:

< ced@comune.senigallia.an.it >

Controllo versione e Cronologia modifiche

Controllo di versione	Data effettiva	Approvato da	Descrizione delle modifiche effettuate
1.0	21/12/2021	DG 313 del 21/12/2021	Prima stesura del REGOLAMENTO PER LA GESTIONE E L'UTILIZZO DEI SISTEMI INFORMATICI E TELEMATICI COMUNALI
1.1	15/07/2026		Integrazione norme sull'IA – Accordo Log di Posta Elettronica – Revisione Generale del Documento

Sommario

Approccio metodologico

L'obiettivo di un ***Regolamento*** è la definizione delle modalità di funzionamento di un sistema organizzativo o tecnologico e della relativa disciplina di utilizzo. Solitamente sono prima declinati i principi generali che hanno richiesto o suggerito la regolamentazione, a cui segue una parte attuativa e l'immancabile sezione relativa alle sanzioni, con gli allegati utili nella comprensione nell'applicazione pratica.

La redazione di un ***Regolamento per l'utilizzo di sistemi e di servizi IT ha come obiettivo primario la definizione delle politiche di sicurezza*** dell'organizzazione in modo da disciplinare:

- le cose che si *possono* fare;
- le cose che si *devono* fare secondo una specifica modalità o procedura;
- quanto *non è* proprio possibile fare.

Da un lato l'organizzazione ha la necessità di normare questo ambito per tutelare il suo patrimonio informativo e per prevenire problemi reputazionali o danni di immagine dovuti ad utilizzi impropri degli strumenti; dall'altro vi è la necessità di sensibilizzare, formare ed informare il personale su tematiche sempre nuove legate al progresso e all'innovazione che, considerati i ritmi evolutivi, crea dei veri e propri dislivelli culturali difficilmente colmabili.

La regolamentazione che segue modifica radicalmente l'approccio tradizionale, introducendo una metodologia più rigorosa e basata sull'analisi dei rischi che incombono sull'organizzazione e sui sistemi informatici, in conformità con le recenti disposizioni normative in materia di sicurezza informatica e protezione dei dati personali.

In modo forse non canonico ma funzionale, si è partiti dalle sorgenti di dati, analizzando le potenziali minacce e vulnerabilità, integrando progressivamente con delle casistiche basate su eventi realmente accaduti. In altre parole, pur mantenendo l'asse sui principi generali, il focus è rivolto alla costruzione di uno strumento che possa fungere da vademecum, con l'obiettivo di educare gli utilizzatori ad un uso consapevole e corretto in modo da ridurre sostanzialmente i rischi che incombono sul patrimonio informativo dell'organizzazione, piuttosto che realizzare un mero dispositivo normativo di repressione delle cattive pratiche.

L'intento del presente documento è avviare un'azione di sensibilizzazione, che migliori le conoscenze legate agli strumenti tecnologici e ai rischi connessi, al fine di arrivare ad una nuova consapevolezza finalizzata alla prevenzione piuttosto che alla cura delle problematiche troppo spesso legate al "*non sapevo*", "*non immaginavo che".* Le sorgenti di rischio provengono dalle Minacce ENISA e dal NIST Risk Management Framework. I pericoli sottesi a tali sorgenti di rischio sono seri e in grado di produrre danni rilevanti in termini di funzionalità dei sistemi, continuità operativa dei servizi e di riservatezza delle informazioni trattate.

Mappa degli articoli del Regolamento IT con i Requisiti ISO/IEC 27001 e D.lgs. 138/2024

In Appendice 5 sono riportate le mappe dei controlli previsti al prospetto A.1 - "Controlli per la sicurezza delle informazioni", previsti dalla norma ISO/IEC 27001:2022, con gli articoli del presente Regolamento; in Appendice 6 sono riportati i requisiti previsti all'Allegato 2 della Det. ACN 2025/164179 e i riferimenti del presente Regolamento.

Articolazione del Regolamento

Il presente Regolamento prevede una prima parte introduttiva dove sono identificate e definite le componenti del sistema di gestione nel suo complesso, a cui segue un elenco che riepiloga per ogni tipologia di servizio o di sistema le corrette modalità di utilizzo. Infine, sono riportati in appendice alcuni validi strumenti atti a ridurre gli errori tipici degli utilizzatori.

CAPO I - Disposizioni generali

Art. 1. - Oggetto e finalità

1) Il Comune di Senigallia è da anni fortemente impegnata in importanti investimenti legati alle tecnologie e ai servizi dell'informazione al fine di supportare le funzioni istituzionali, unite alle attività amministrative e di gestione dei servizi.
   Il presente Regolamento definisce il modello comportamentale considerato accettabile, per gli utilizzatori dei servizi e dei sistemi informatici dell'organizzazione e, inoltre, rappresenta idonea informativa ai sensi della vigente disciplina sulla protezione dei dati personali per quei trattamenti connessi con le attività di monitoraggio e controllo comunicata da parte del Titolare.
2) Al fine di preservare il patrimonio informativo dell'organizzazione, la continuità operativa dei servizi erogati e parallelamente ridurre i rischi di esposizione, sia dal punto di vista sanzionatorio che risarcitorio (tenuto conto delle normative nazionali ed europee vigenti, come il GDPR o il D.lgs. 138/2024), il Comune di Senigallia richiede agli utilizzatori dei servizi e dei sistemi informatici di conformarsi obbligatoriamente ai dettami del presente Regolamento.

Art. 2. - Ambito di applicazione - Perimetro

1) Il presente Regolamento si applica a tutti gli utilizzatori dei sistemi e dei servizi IT dell'organizzazione compresi nel perimetro, corrispondente alla massima estensione della rete di comunicazione privata fino al firewall di connessione con la rete pubblica, includendo anche i sistemi collegati via Virtual Private Network (VPN) e i sistemi posizionati in zone demilitarizzate (DMZ), in *colocation*, in *hosting*, in *housing* o in cloud.
2) Sono compresi tutti gli elementi della catena tecnologica come le *facility*, il network, i sistemi server, il *middleware*, le applicazioni software come anche i sistemi di gestione della sicurezza, il monitoraggio e il controllo, i dispositivi client (come i personal computer, i *thin client*, le stampanti multifunzione, i centralini telefonici, i telefoni basati su tecnologia IP, gli smartphone e i tablet) o dispositivi *edge* (come dispositivi medici e strumenti scientifici, veicoli a guida autonoma e macchine automatizzate, ovvero ogni "cosa" che fa parte dell'*Internet of Things*).
3) Sono escluse dal perimetro tutte le reti Wi-Fi di tipo *guest* (ad accesso gratuito per il pubblico) e gli eventuali dispositivi collegati.
4) Gli utilizzatori dei servizi pubblicati e accessibili dalla rete Internet sono esclusi dal perimetro (ad esempio, sono esclusi coloro che visitano i siti web istituzionali o la sezione relativa agli obblighi di amministrazione trasparente).

Art. 3. - Applicazione del Regolamento IT

1) Gli utenti sono obbligati ad accettare e a conformarsi al presente Regolamento come condizione necessaria per l'accesso e l'utilizzo dei servizi e dei sistemi IT.
2) Il rispetto delle prescrizioni è il prerequisito per un impiego legittimo e ottimale dei servizi e dei sistemi IT, sia per il personale deputato alla gestione che per tutti gli utilizzatori.

Art. 4. - Definizioni

Ai fini del presente Regolamento s'intende per:

1) **Minaccia**: elemento potenzialmente pericoloso; possibile evento non desiderato che porta alla perdita di riservatezza, integrità o disponibilità delle informazioni;
2) **Vulnerabilità**: caratteristica dei sistemi e dei processi che identifica una fragilità, un punto debole che, in particolari condizioni, può comportare la perdita di riservatezza, integrità o disponibilità delle informazioni;
3) **Contromisure:** azioni di prevenzione e mitigazione delle vulnerabilità individuate al fine di limitare i rischi di perdita di riservatezza, integrità o disponibilità delle informazioni;

4) **Rischio:** probabilità che un evento si verifichi ovvero che una minaccia si trasformi in evento indesiderato e dannoso sfruttando una vulnerabilità;
5) **Fonte di rischio:** elemento tangibile o intangibile che possiede il potenziale intrinseco di originare il rischio singolarmente o in combinazione con altri elementi;
6) **Evento sfavorevole:** particolare insieme di circostanze in grado di modificare in modo negativo e contrario rispetto al normale comportamento di un sistema, ambiente, processo, flusso di lavoro o di una persona;
7) **Conseguenza:** effetto diretto o indiretto di un evento;
8) **Incidente alla sicurezza:** evento volontario o involontario attribuibile a una o più persone con associato un costo economico diretto (es. sostituzione del bene e interruzione del servizio) oppure indiretto (uso non autorizzato di informazioni, violazioni di legge, danni di immagine e reputazionali) che comporta una minaccia alla sicurezza;
9) **Impatto (negativo):** stima delle potenziali perdite dirette o indirette associate a un rischio;
10) **Credenziali di autenticazione:** codice per l'identificazione dell'utilizzatore di un sistema o di un dispositivo associato a una parola chiave riservata, conosciuta solamente dal soggetto (spesso identificata come coppia login o codice utente e password) e che lo identificano univocamente;
11) **Spam:** ovvero spazzatura spesso associata alla posta elettronica (in inglese *junk e-mail*) che indica la ricezione di messaggi spesso indesiderati, ripetuti o monotematici (es. pubblicità) il cui mittente spesso è sconosciuto.

Art. 5. - Principi

1) I principi ispiratori del presente Regolamento sono i seguenti:
   a) Tutela dei diritti, delle libertà e della dignità delle persone;
   b) Garanzia della necessaria *continuità operativa* per l'erogazione del miglior servizio possibile unito al minor dispendio di energie (umane, tecnologiche, temporali ed economiche);
   c) Tutela del patrimonio informativo dell'organizzazione e riduzione dei rischi connessi al trattamento dei dati e quindi della probabilità di:
      i. accessi illegittimi ai sistemi o agli applicativi;
      ii. modifiche indesiderate alle informazioni;
      iii. perdita della disponibilità dei dati;
   d) Conformità normativa e allineamento agli standard di mercato;
   e) *Security* e *privacy by design,* ovvero sicurezza e conformità alla protezione dati personali come parte integrante della progettazione complessiva e governo del sistema;
   f) *Security* e *privacy by default*, ovvero progettazione e configurazione dei sistemi e delle applicazioni software in modo da garantire il massimo livello di sicurezza possibile, fin dalla prima installazione e senza particolari interventi attivi da parte dell'utente;
   g) Approccio alla sicurezza di tipo multilivello (*Layered security*), implementato su livelli differenti ovvero fisico, tecnico, amministrativo, umano, al fine di prevenire, rilevare, contenere e rispondere adeguatamente agli attacchi informatici;
   h) Protezione del patrimonio informativo in ogni fase del trattamento e per tutto il ciclo di vita, ovvero nelle fasi nelle quali i dati sono elaborati e comunicati ("*in transit*") o quando sono conservati ("*in storage*");
   i) Applicazione del modello "*tutto chiuso*" (cd. *default deny all*), ovvero negazione di default degli accessi a sistemi, file, servizi, reti o dati se non esplicitamente autorizzati, comunicazioni di rete con apertura delle sole porte, protocolli e indirizzi strettamente necessari, profili di autorizzazione nelle applicazioni software limitati alle sole operazioni minime necessarie (principio del *need to know* e del *need to do*);
   j) Riduzione della superficie di esposizione rispetto alle vulnerabilità, ovvero alle eventuali debolezze dei sistemi, processi, applicazioni software, hardware, configurazioni o persone che

possono essere sfruttate da una minaccia per compromettere la riservatezza, integrità o disponibilità delle informazioni;

k) Corretto bilanciamento tra usabilità e sicurezza, adottando contromisure basate sull'Analisi dei rischi;
l) Adozione della Regola del minimo previlegio rispetto alla finalità (*separation of duties policy*), in ottica di stratificazione dei profili e degli accessi;
m) Diritto alla disconnessione degli utilizzatori dai sistemi *mobile* al di fuori dell'orario di lavoro;
n) Consapevolezza di tutti gli utilizzatori rispetto ai rischi che incombono sul patrimonio informativo e alle corrette modalità di utilizzo dei sistemi e dei servizi IT.

Art. 6. - Condotta e utilizzo etico dei servizi e dei sistemi IT

2) I sistemi e i servizi IT sono forniti agli utenti per condurre e supportare la missione dell'organizzazione, relativamente agli ambiti tecnici ed amministrativi.
3) Gli utenti sono responsabili dell'utilizzo dei sistemi e dei servizi IT in modo eticamente corretto, sicuro, legale e conforme al presente Regolamento, tenendo nella massima considerazione i diritti, le libertà fondamentali, la sensibilità delle persone come anche gli obiettivi primari dell'organizzazione.
4) L'utilizzatore di sistemi e servizi IT è direttamente responsabile di tutte le attività effettuate con gli *account* dell'organizzazione assegnati, con particolare riguardo alle informazioni inviate o richieste, caricate o visualizzate nel proprio personal computer, applicativo software o piattaforma web dell'organizzazione e non.
5) All'utilizzatore di sistemi e servizi IT sono tassativamente vietate le seguenti attività:
    a. La creazione o la trasmissione di qualsiasi materiale o documento, in qualsiasi formato, che possa essere ragionevolmente ritenuto offensivo, diffamatorio o osceno;
    b. La creazione o la trasmissione di materiale o documento in qualsiasi formato che possa ragionevolmente essere ritenuto suscettibile di molestare, intimidire, danneggiare o turbare qualcuno o qualcosa;
    c. La trasmissione non autorizzata di documenti etichettati come confidenziali su canali o sistemi non sicuri o non omologati dai Sistemi Informativi dell'organizzazione;
    d. L'invio di dati di tipo sensibile su canali non sicuri (un esempio di strumento da evitare per inviare dati sensibili è la posta elettronica dell'organizzazione, che potrebbe viaggiare in chiaro quando inviata ad altro dominio di posta; è da ritenersi invece accettabilmente sicuro l'invio ad altro utente di posta dello stesso dominio. In caso di dubbi è necessario contattare i Sistemi Informativi dell'organizzazione o adottare tecniche di criptazione con invio della chiave su altro canale);
    e. La creazione o la trasmissione di qualsiasi documento non riconducibile alle funzioni o ai compiti di competenza oppure estraneo alle attività dell'organizzazione;
    f. L'accesso non autorizzato ai sistemi o ai servizi IT;
    g. L'utilizzo a fini personali dei sistemi, dispositivi o servizi forniti dall'organizzazione.
6) Gli utilizzatori di sistemi e servizi IT non sono autorizzati a rispondere a interviste telefoniche o sondaggi, compilare questionari on-line (anche quando sollecitati da importanti *brand*).
7) L'introduzione degli strumenti *mobile* (forniti dall'organizzazione o di proprietà personale) pone il problema dell'equilibrio tra vita privata e vita professionale, data la progressiva trasformazione degli strumenti di comunicazione da asincroni a tempo reale. È riconosciuto all'utilizzatore il diritto

alla disconnessione[1] dai dispositivi *mobile* al di fuori dell'orario di lavoro e dai turni di pronta disponibilità o reperibilità.

8) Anche nel caso dei sistemi di *instant messaging* (es. WhatsApp) vale il diritto alla disconnessione; è demandato alla sensibilità dei singoli il rispetto della distinzione tra tempistiche professionali e momenti da dedicare alla vita privata e familiare.

Art. 7. - Tipologie di minacce

1) Una prima classificazione delle minacce è riconducibile all'elemento sorgente o alla causa:
   - Deliberata o Intenzionale;
   - Accidentale (come perdite involontarie di informazioni o risorse IT);
   - Naturale.
2) In funzione delle tipologie di minacce è necessario attivare tutte le opzioni possibili al fine di ridurre la superficie di esposizione; l'organizzazione e la relativa profilazione dell'utenza è uno dei possibili elementi di attenuazione per quanto riguarda gli attacchi deliberati, mentre per gli eventi accidentali o legati all'inconsapevolezza dei comportamenti a rischio degli operatori è fondamentale un'azione prima di tutto culturale, volta alla sensibilizzazione al tema della sicurezza delle informazioni. Per quanto attiene alle minacce naturali è invece necessario agire sulle infrastrutture e sulla catena tecnologica con adeguati elementi di ridondanza.

Art. 8. - Sistema di gestione della sicurezza dell'informazione

1) Un Sistema di Gestione della Sicurezza dell'Informazione (SGSI o ISMS secondo la norma ISO 27001), è un insieme di politiche e procedure per la gestione sistematica delle informazioni trattate dall'organizzazione. L'obiettivo di un SGSI è ridurre al minimo i rischi e garantire la continuità operativa dell'organizzazione agendo sugli aspetti di sicurezza logica, fisica ed organizzativa, al fine di limitare proattivamente l'eventuale impatto di una violazione.
2) Il presente Regolamento IT, unitamente alle previste procedure IT, alla modulistica e alle linee guida, sono parte integrante del SGSI.
3) Le procedure IT e la manualistica relativa sono pubblicate, nella versione aggiornata, nella intranet dell'organizzazione sezione formazione.

CAPO II - Strumenti

Art. 9. - Identificazione, autenticazione e autorizzazione

1) L'organizzazione implementa, nella gestione dei sistemi e dei servizi IT, la famiglia di protocolli "AAA", basata sulle funzioni di Autenticazione, Autorizzazione e *Accounting* (v. articolo successivo).
2) Quanto previsto in questa sezione non si applica ai servizi pubblici, che non richiedono autenticazione e ai sistemi ad alta rotazione e intensità (es. Front Office, ecc.) dove possono essere previsti *account* di accesso multiutente (cosiddetti *account* generici); successivamente sono comunque tracciate le singole attività eseguite a livello di applicazione software (*application log*).
3) L'accesso alla rete e ai sistemi dell'organizzazione è possibile soltanto se l'utilizzatore:
   a) È stato prima di tutto ***identificato*** ovvero sono conosciute le sue generalità ed è stato dotato di credenziali utente (nome utente, password e/o PIN), soggette alle condizioni previste in questa sezione del Regolamento;

[1] Legge 6 maggio 2021, n. 61, di conversione del decreto-legge 13 marzo 2021, n. 30 riconosce esplicitamente al dipendente che lavora in modalità agile (o smart working) il diritto di disconnettersi dalle strumentazioni tecnologiche e dalle piattaforme informatiche utilizzate per svolgere la prestazione lavorativa.

b) Effettua l'***autenticazione*** tramite immissione delle credenziali, in modo che il sistema possa verificare se l'individuo è chi sostiene di essere, permettendone univoca identificazione;
c) È stato ***autorizzato*** ovvero è stato conferito il diritto ad accedere a specifiche risorse in base al ruolo ricoperto, al profilo e alle specifiche mansioni assegnate.

4) La responsabilità delle azioni effettuate utilizzando la coppia "nome utente e password e/o PIN" sarà attribuita in termini di responsabilità al soggetto titolare dell'*account*, a meno di comprovato illecito da parte di terzi. Sono escluse le attività di supporto autorizzate dagli stessi utilizzatori per interventi di manutenzione o assistenza tecnica.
5) **Gli *account* di accesso del personale dipendente, dei consulenti esterni e dei fornitori sono di tipo nominativo e non riutilizzabile da altri soggetti, anche dopo la conclusione del rapporto di lavoro.**
6) Gli *account* di accesso hanno, per impostazione predefinita, una scadenza corrispondente alla data di fine del contratto, convenzione o accordo. È a carico del Dirigente Responsabile comunicare al personale dei Sistemi Informativi l'eventuale prolungamento del contratto e la necessità di estensione temporale delle autorizzazioni (attività obbligatoria nel caso di mancata copertura da parte del sistema di gestione delle identità, direttamente integrato con il gestionale HR).
7) Il personale dei Sistemi Informativi specificatamente autorizzato gestisce gli *account* utente per tutto il ciclo di vita tramite apposita procedura (creazione, aggiornamento, nuovi profili di autorizzazione, reset della password, verifica periodica dell'ambito di autorizzazione, disattivazione una volta concluso il rapporto di lavoro).
8) La normativa vigente in tema di sicurezza IT e protezione dei dati, le norme volontarie e le *best practice* di settore impongono di stratificare le possibilità di accesso ai sistemi e ai servizi IT al fine di garantire un adeguato livello di sicurezza. Ad ogni *account* utente è collegato uno specifico *profilo di autorizzazione* che permette al singolo utilizzatore l'accesso in funzione del proprio ruolo, delle attività a cui è delegato e specificatamente autorizzato da un superiore (o soggetto Designato ai sensi del D.lgs. 196/03 e ss.mm.ii.). Le eventuali estensioni o eccezioni devono essere autorizzate e tracciate secondo procedura dedicata.
9) Il sistema di Autenticazione, Autorizzazione e Registrazione degli accessi ha l'obiettivo di garantire un adeguato livello di sicurezza, conforme a quanto previsto dalla normativa vigente e dal presente Regolamento, poiché traccia, separa gli accessi nei livelli previsti, tutelando la riservatezza e l'integrità delle informazioni trattate.
10) La politica di sicurezza dell'organizzazione prevede, per alcune tipologie di servizi, la necessità di accesso tramite autenticazione a più fattori (MFA), utilizzando una delle modalità previste dalla *mobile* app dedicata (QR-Code, PIN, OTP temporaneo).

Art. 10. - Registrazione delle attività (*Accounting*)

1) A partire dall'accesso ai sistemi o ai dispositivi, le attività degli utilizzatori sono registrate in appositi file detti di *log*. Nei sistemi critici, di particolare rilevanza o di fede privilegiata sono memorizzate tutte le singole attività svolte riportando *account* utente, indirizzo o nome macchina, ora, data e il dettaglio delle azioni svolte, incluso il protocollo di comunicazione utilizzato.
2) Al fine di contenere lo spazio necessario alla conservazione, i file di log sono conservati in logica di rotazione, ovvero sono sovrascritti al raggiungimento di una certa data o di una certa dimensione, a meno della cosiddetta prevista *retention* dei sistemi di backup; in ogni caso la conservazione è strettamente limitata al perseguimento delle finalità organizzative, produttive e di sicurezza.
3) I file di log sono conservati per il tempo **strettamente necessario** al perseguimento delle finalità di sicurezza e gestione dei sistemi, secondo criteri di proporzionalità e minimizzazione.
4) L'eventuale prolungamento dei tempi di conservazione è valutato sempre come eccezione, attuabile soltanto in relazione:

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

5) Il connesso trattamento di dati personali è comunque limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed è effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità.
6) I controlli di tipo indiretto, così come stabilito dalla disciplina sui controlli a distanza dei lavoratori[2], e i connessi trattamenti di dati personali lecitamente effettuabili dal datore di lavoro, sono comunque configurati in modo graduale, previo esperimento di misure comunque atte a garantire i diritti degli interessati, escludendo attività idonee a realizzare controlli di tipo massivo, prolungato e indiscriminato dell'attività del dipendente stesso.
7) L'accesso ai log è consentito al solo personale, espressamente autorizzato e nominato amministratore di sistema [Garante Privacy 27 novembre 2008 doc. web n. 1577499] e adeguatamente istruito in materia di protezione dei dati personali, nel rispetto del principio di limitazione della finalità.

Art. 11. - Corretto uso delle Credenziali di autenticazione

1) Le credenziali di autenticazione sono composte da un codice (*account* utente) facilmente riconducibile al soggetto e da una *password e/o PIN conosciuti al solo utilizzatore*. ***È tassativamente vietato rivelare la propria password*** di accesso alla rete, agli applicativi o servizi disponibili (inclusi le piattaforme regionali o ministeriali), anche a terzi autorizzati. Qualsiasi azione effettuata utilizzando la coppia "*account* utente e password e/o PIN" sarà attribuita in termini di responsabilità all'utente titolare registrato, a meno di comprovato illecito da parte di terzi.
2) La *lunghezza minima della password,* in presenza di autenticazione MFA, deve essere di almeno 12 caratteri; considerato che i sistemi di violazione impiegano tempistiche esponenzialmente proporzionali con la lunghezza della password da violare, è necessario considerare almeno 14 caratteri[3] per gli *account* dei servizi on-line (es. posta elettronica, piattaforme web) e per gli *account* qualificati amministrazione di sistema, non collegati ad un sistema MFA.
3) Le password non devono essere trascritte; per questo è importante che siano facili da ricordare. È consigliabile utilizzare delle tecniche di memorizzazione (ad es., "Mi_P1@c3_l4_P1zz@").
4) È fondamentale utilizzare password diverse per scopi, piattaforme o applicativi software diversi. In caso contrario, sussiste il rischio (non remoto) che l'eventuale violazione di un sistema possa comportare effetti indesiderati anche su tutti gli altri sistemi utilizzati, dell'organizzazione e ad uso personale, riconducibili allo stesso soggetto.
5) Le password devono essere modificate ad intervalli regolari per ridurre l'eventuale finestra temporale di esposizione e comunque almeno ogni 4 mesi (cd. *Password aging*).
6) Le password non devono mai far riferimento a termini di senso compiuto poiché già contenute nei dizionari utilizzati dai sistemi di violazione, oppure essere troppo ovvie (ad es., 'P@ssword').
7) Le password non devono essere in alcun modo collegate alla vita privata o lavorativa dell'utilizzatore. Sono quindi da escludere i nominativi dei familiari, la data di nascita, il codice identificativo, la targa dell'auto, la squadra del cuore, il soprannome, ecc. (il precedente elenco non è esaustivo).

[2] Art. 4, l. 20.5.1970, n. 300 – Statuto dei lavoratori, incluse modifiche disposte dall'art. 23 del D.lgs. 151/2015
[3] Misura minima prevista da AgID - «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)». (17A03060) (GU Serie Generale n.103 del 05-05-2017)

8) Le password devono rispettare i criteri di complessità definiti dai sistemi informativi dell'Ente. In particolare, le password devono avere una lunghezza minima stabilita dalle politiche di sicurezza ed essere composte da caratteri appartenenti ad almeno tre delle seguenti categorie: lettere maiuscole, lettere minuscole, numeri e caratteri speciali.
9) Le password non devono inoltre contenere il nome dell'account utente né parti significative del nome e cognome dell'utilizzatore.
10) Le password non devono essere riutilizzate a breve distanza di tempo; la rotazione minima prevista è almeno pari a 5 password diverse consecutive (cd. *Password history*);
11) Le password degli *account* di accesso ai sistemi non sottoposti alle politiche di complessità, di invecchiamento o di rotazione impostate nel sistema di autenticazione centrale, devono comunque rispettare le medesime regole, agendo manualmente.
12) Le password e i PIN non devono essere comunicate a nessuno, per nessun motivo, con nessun mezzo (ad esclusione del primo accesso o primo invio). In caso di problemi di accesso alle risorse fare riferimento al supporto tecnico.
13) La digitazione delle password deve avvenire in massima sicurezza, evitando di mostrare a terzi la sequenza dei tasti premuti. I colleghi impegnati in attività condivise al computer sono tenuti a voltarsi nel caso sia richiesta l'autenticazione al sistema o alla piattaforma software utilizzati.
14) È consentita la memorizzazione delle password all'interno dei browser web aziendali (ad es. Google Chrome, Microsoft Edge), solo se l'accesso prevede un secondo fattore di autenticazione MFA, in quanto l'accesso, la visualizzazione o la copia delle credenziali memorizzate sono protetti dall'autenticazione dell'utente tramite le credenziali di dominio del sistema. È invece vietata la memorizzazione delle password tramite applicativi di gestione password non espressamente autorizzati o distribuiti dai Sistemi Informativi. Sono altresì esclusi sistemi o applicativi software di memorizzazione delle credenziali basati su servizi cloud, salvo diversa indicazione e autorizzazione da parte dei Sistemi Informativi.
15) Non utilizzare strumenti web per la generazione o il controllo del livello di sicurezza (utilizzare eventualmente password con costruzione simile e al solo fine di verificarne la robustezza).
16) Per l'invio delle password di criptazione dei file e della documentazione non utilizzare mai lo stesso canale (es. file criptato inviato via posta elettronica e password comunicata a voce, via telefono).
17) Non seguire le mode del momento, utilizzare acronimi, *pattern* ('CristianoRonaldo$' oppure sempre il primo carattere di ogni parola maiuscolo e un dollaro finale), ripetizioni e sequenze ('11111Paperin0000' oppure 'QWERTY12345') o parole presenti nei dizionari (in Appendice 1 - Password presenti nei dizionari pubblici sono riportate degli esempi di password da NON utilizzare).
18) Nel caso di perdita (o anche solo del sospetto di perdita) della segretezza della password è necessario:
    a. Modificare immediatamente la password in uso (sui sistemi Windows CTRL+ALT+CANC e "Cambia password"; verificare le modalità per i singoli applicativi software con autenticazione locale) oppure tramite la funzione online cambia password disponibile nella intranet aziendale cas.comune.senigallia.an.it;
    b. Comunicare l'accaduto ai Sistemi Informativi dell'organizzazione, al proprio Responsabile, al CISO e al Privacy Officer / DPO per la valutazione della gravità della situazione e l'attivazione delle procedure di emergenza per incidente alla sicurezza, al fine di attivare tutti i controlli e le contromisure del caso.
19) Per gli accessi ai servizi cloud, il sistema di autenticazione Microsoft AZURE ID applica meccanismi automatici di protezione denominati Smart Lockout che prevedono, secondo la configurazione vigente, il blocco temporaneo dell'autenticazione a seguito di tentativi di accesso errati ripetuti. Attualmente il **blocco viene applicato dopo 10 (dieci) tentativi** consecutivi non riusciti e ha una durata iniziale di sessanta secondi. Tali meccanismi operano secondo criteri adattivi di sicurezza e non si basano su soglie rigide tipiche dei sistemi di dominio tradizionali. Il blocco temporaneo

dell'autenticazione viene rimosso automaticamente allo scadere del periodo previsto, senza necessità di intervento amministrativo; l'utente può quindi riprovare l'accesso trascorso il tempo di blocco.

20) Nei casi di particolare emergenza oppure in presenza di comportamenti che possano comportare problemi di sicurezza, i Sistemi Informativi sono autorizzati alla momentanea disattivazione dell'*account* e isolamento del sistema utilizzato. Risolta la problematica evidenziata sarà cura dei Sistemi Informativi ripristinare le precedenti funzionalità e autorizzazioni.
21) Le richieste di cambiamento o reset password dell'*account* di accesso ai sistemi dell'organizzazione non sono mai inviate tramite e-mail. Eventuali e-mail che richiedano tramite link la modifica della password devono essere marcate come spam e cestinate.
22) È tassativamente vietato memorizzare *account* di accesso ai sistemi e servizi dell'organizzazione in documenti salvati in sistemi o dispositivi al di fuori del perimetro dell'organizzazione e ad accesso pubblico, inclusi sistemi di file hosting (come Google Drive o Dropbox).
23) Gli *account* di amministrazione di dominio possono essere utilizzati soltanto nei client assegnati al personale dei Sistemi Informativi o posizionati nel data center; questo al fine di evitare problemi di registrazione delle password attraverso *keylogger*, di tipo hardware o software.

Art. 12. - Posta elettronica convenzionale

1) La posta elettronica è uno strumento di comunicazione e deve essere utilizzato soltanto per effettuare corrispondenze legate al servizio svolto nell'organizzazione, anche nel caso di *account* di posta elettronica di tipo nominativo. In nessun caso sono previsti indirizzi di posta elettronica ad uso privato.
2) La politica di comunicazione con soggetti esterni all'organizzazione prevede, specie in ricezione, l'utilizzo preferenziale di indirizzi di posta elettronici condivisi tra più utilizzatori (cd. *liste di distribuzione),* come ad es. <ufficio>@<dominio.it>; in tale modalità il messaggio è inviato al relativo gruppo di utilizzatori e non sono necessarie modifiche o particolari procedure in caso di *turnover* del personale.
3) Ogni utilizzo della posta elettronica deve essere effettuato coerentemente con le politiche e le procedure dell'organizzazione nel rispetto dell'etica, della sicurezza e in piena conformità alle leggi applicabili.
4) L'utilizzatore è tenuto a controllare almeno una volta a giorno il proprio *account* di posta elettronica per verificare l'eventuale arrivo di nuovi messaggi e conseguentemente l'assegnazione di specifici compiti.
5) La posta elettronica dell'organizzazione è erogata tramite piattaforma Microsoft 365 ed è utilizzabile:
   – in modalità web tramite browser;
   – tramite il client di posta elettronica ufficiale fornito da Microsoft 365, installato sui personal computer assegnati dall'organizzazione e gestiti dai Sistemi Informativi.
6) È consentito esclusivamente l'utilizzo del client Microsoft ufficiale, correttamente licenziato e configurato secondo le policy di sicurezza dell'organizzazione.
   È tassativamente vietato l'utilizzo di software di terze parti per la gestione della posta elettronica (a titolo esemplificativo e non esaustivo: Thunderbird, client open source, applicazioni non ufficiali o non omologate), nonché l'installazione autonoma di applicativi di posta non autorizzati.
   L'installazione, configurazione e aggiornamento del client di posta elettronica Microsoft 365 sono a carico dei Sistemi Informativi dell'organizzazione.
   Eventuali deroghe devono essere motivate, formalmente autorizzate dal Responsabile di Area e validate dai Sistemi Informativi, nel rispetto delle misure di sicurezza e protezione dei dati personali previste dal presente Regolamento.

7) La posta elettronica non deve essere utilizzata per la creazione, distribuzione o rilancio di messaggi di disturbo o offensivi, commenti sull'origine razziale o etnica, sulle opinioni politiche, sulle convinzioni religiose o filosofiche, o sull'appartenenza sindacale, sullo stato di salute o sulla disabilità, sul genere, sul colore dei capelli, sull'età, sulla vita o sull'orientamento sessuale della persona. I dipendenti che dovessero ricevere messaggi con queste tipologie di contenuto da qualsiasi dipendente devono segnalare immediatamente il fatto al diretto superiore.
8) La posta elettronica non deve essere utilizzata per inviare messaggi massivi ad una moltitudine di utenti, in particolare per diffondere locandine, inviti o pubblicizzare eventi, prediligendo la pubblicazione sulla intranet dell'organizzazione nella sezione *news* o eventi, a meno di informazioni particolarmente importanti o urgenti, e comunque su specifica autorizzazione della Direzione.
9) L'utilizzatore non può utilizzare la posta elettronica dell'organizzazione per inviare documenti contenenti dati personali, specie se di natura particolare, che lo riguardano o che riguardino soggetti terzi.
10) **L'utilizzatore non deve mai inserire nell'oggetto del messaggi dati personali e dati particolari che trattano ad esempio origine razione, credo religioso, appartenenza politica** ecc
11) Il Regolamento (UE) 2014/910 eIDAS (*electronic IDentification Authentication and Signature*) e le conseguenti modifiche al D.lgs. 82/2005 (Codice dell'Amministrazione Digitale - CAD), nonché i recenti orientamenti giurisprudenziali[4], prevedono per la posta elettronica ordinaria validità giuridica e rilevanza probatoria[5], liberamente valutabile in giudizio tenuto conto delle caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.
12) Un messaggio di posta elettronica convenzionale inviato allo stesso dominio ("@comune.senigallia.an.it") ha un livello di sicurezza mediamente elevato; nel caso di invio ad altri domini di posta anche se istituzionali (ministeri, regioni, comuni, ecc.) non è purtroppo garantito un corrispondente livello di sicurezza, in taluni casi equiparabile addirittura alla semplice cartolina postale. Per questo motivo è necessario verificare sempre, prima dell'invio, il destinatario (soprattutto se multiplo) e il contenuto della comunicazione (oggetto, testo e allegati).
13) Alla fine della sessione di lavoro è necessario effettuare sempre la disconnessione (*log-out*) dal sistema di posta elettronica.
14) L'indirizzo di posta elettronica non deve essere utilizzato per la registrazione a siti web o piattaforme applicative che non siano in qualche modo legate alle attività svolte dagli utilizzatori intestatari nell'organizzazione (questa indicazione permette di limitare il traffico di spam a monte).
15) Non fare mai click sui link di annullamento alle sottoscrizioni delle e-mail considerate indesiderate (cd. "*unsubscribe*"), in modo da evitare la conferma dell'esistenza e utilizzo dell'account e-mail.
16) Al fine di garantire la dovuta coerenza nella comunicazione, è vietato modificare il *footer* (parte finale del messaggio di *default*) rispetto allo standard dell'organizzazione.
17) Tutti i messaggi di posta elettronica devono riportare in calce la firma del mittente secondo lo standard dell'organizzazione, con font e dimensioni come di seguito riportato:

Rossi Mario	[font Calibri 11 punti in **grassetto**]
Ruolo e Unità operativa di appartenenza	[font Calibri 10 punti normale]
Denominazione Organizzazione	[font Calibri 10 punti normale]
Indirizzo	[font Calibri 10 punti normale]
Telefoni (fisso e mobile organizzazione)	[font Calibri 10 punti normale]

[4] Sentenze n. 14716/2011 e n. 11402/2016 Tribunale di Milano

[5] Dalla definizione CAD di "firma elettronica: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica", l'utilizzo delle credenziali di accesso alla casella di posta elettronica vale a qualificare l'utente e costituisce pertanto una firma elettronica semplice, non avanzata né qualificata, ma comunque non giuridicamente irrilevante e sotto il profilo probatorio liberamente valutabile in giudizio

Non sono ammesse personalizzazioni differenti o l'aggiunta di ulteriori immagini grafiche, specie se di grandi dimensioni.

18) I sistemi di sicurezza attivi come firewall e antispam garantiscono con discreta probabilità che le e-mail consegnate siano esenti da pericoli. È comunque a carico dell'utilizzatore la verifica ultima di:
    a. **Mittente**: deve essere conosciuto (da verificare l'indirizzo effettivo e non la semplice denominazione); esempio da evitare e marcare come spam è il mittente mario@acme.com con indirizzo effettivo service145@mail.145.com;
    b. **Link**: i link devono essere verificati prima di essere lanciati (fare click) anche nel caso appaiano a prima vista del tutto familiari (soprattutto per l'aspetto grafico) al fine di evitare attacchi di tipo *phishing*; la verifica può essere fatta posizionando il cursore del mouse sul link per visualizzare la reale destinazione (ad esempio evitare di fare click su link del tipo http://amazon.net.ru);
    c. **Allegati**: diffidate dei file con estensione multipla, senza estensione o con denominazione estranea alle attività o mansioni svolte abitualmente (ad es., '*Si allega fattura*');
    d. **Contenuti**: scrittura con errori grossolani (traduzione da sistemi automatici), riferimenti alla chiusura di un conto o di un servizio, parole come "URGENTE" o "IMMEDIATO", richieste di dati personali o di password, file che non sono mai stati richiesti o con estensioni sconosciute o sospette.
19) Nei casi dubbi non aprire le e-mail o gli allegati e contattare il supporto tecnico che provvederà alla verifica secondo le corrette procedure di sicurezza.
20) È vietato il *forward* o rilancio della posta sui dispositivi mobili (es. smartphone e tablet) personali. L'apertura dei messaggi di posta elettronica è permessa solamente sui dispositivi mobili di proprietà dell'organizzazione, agli utilizzatori specificatamente autorizzati.
21) L'utilizzo di *forward* automatico di posta elettronica dell'organizzazione su altri sistemi (es. Gmail) è vietato; questo al fine di garantire un adeguato livello di sicurezza dei contenuti come, ad esempio, gli allegati contenenti dati personali o riservati inviati dal mittente che, non essendo a conoscenza del rilancio, non adotta le misure necessarie alla protezione dei contenuti prevista per trasferimenti al di fuori dell'Unione Europea.
22) La posta elettronica fornita dall'organizzazione non può essere utilizzata per scopi personali estranei all'attività lavorativa. Viceversa, è vietato utilizzare o fornire e-mail personali per scambiare informazioni, contenuti o allegati connessi all'attività lavorativa.
23) Non consultare la posta elettronica dell'organizzazione presso Internet point, Wi-Fi pubblici o sistemi di connettività condivisa (es. alberghi, ristoranti, bar) al fine di ridurre rischi legati all'esfiltrazione delle credenziali; prediligere la connettività 3G/4G/5G del proprio dispositivo *mobile*.
24) Eventuali raccomandazioni o indicazioni ricevute via e-mail, anche da soggetti conosciuti, non devono essere seguite poiché nella maggior parte dei casi si tratta di virus di tipo HOAX (cd. bufale). In caso di dubbi contattare sempre il supporto tecnico.
25) Marcare sempre come spam le e-mail che appaiono come *scam* ovvero tentativi di truffa pianificata con metodi di ingegneria sociale (in genere nella e-mail si promettono enormi guadagni in cambio di somme di denaro da anticipare).
26) Le e-mail che richiedono l'attivazione delle macro di MS-Word o MS-Excel prima del download degli allegati devono essere immediatamente marcate come spam.
27) Non attivare mai i link presenti nelle cosiddette e-mail di reset della password, né fornire mai le credenziali di autenticazione per nessun motivo.
28) Non rispondere e inoltrare e-mail delle cosiddette catene di Sant'Antonio o rispondere alle e-mail di spam.

29) Le funzionalità e i limiti della posta elettronica variano in funzione del profilo di licenza Microsoft 365 assegnato all'utente. In particolare, agli utenti con licenza Microsoft 365 E3 è assegnata una casella di posta elettronica con capacità fino a 100 GB, adeguata a un utilizzo continuativo degli strumenti digitali, mentre agli utenti con licenza Microsoft 365 F3 è assegnata una casella di posta elettronica con capacità fino a 2 GB, destinata a un utilizzo operativo ed essenziale del servizio. In ogni caso, deve essere evitata la trasformazione del sistema di posta elettronica in un sistema di archiviazione; gli utenti sono pertanto tenuti a procedere con periodiche cancellazioni dei messaggi non più utili.
30) La dimensione massima dei messaggi di posta elettronica, inclusi gli allegati inviati o ricevuti, è soggetta alle limitazioni tecniche della piattaforma Microsoft 365 ed è attualmente pari a 33 MB e un limite massimo di 250 allegati. Il superamento di tali limiti viene automaticamente impedito dal sistema in fase di invio del messaggio.
31) Gli allegati inviati via e-mail contenti dati personali o riservati devono essere criptati adottando le procedure e le modalità previste in questi casi. La password di decriptazione deve essere comunicata al destinatario con altro mezzo (ad es., via telefono).
32) Le e-mail contenenti evidenze di reati devono essere prima visionate dal personale tecnico dei Sistemi Informativi e poi, se del caso, informate le autorità per la presentazione della denuncia; tale procedura è finalizzata ad evitare falsi allarmi.
33) L'invio a più soggetti di un messaggio di posta elettronica può essere effettuato in "CC" (*Carta Carbone*) soltanto nel caso di destinatari appartenenti allo stesso dominio di posta (@comune.senigallia.an.it); nel caso di invio a più destinatari è FONDAMENTALE utilizzare il "CCN" (*Carta Carbone Nascosta*) in modo che i singoli non possano in nessun modo venire a conoscenza degli indirizzi degli altri destinatari.
34) L'invio di messaggi di posta elettronica a sottogruppi numerosi oppure a tutti i destinatari del dominio di posta è riservato ai soggetti specificamente autorizzati. Eventuali forzature del sistema potranno essere sanzionate ai sensi del presente Regolamento.
35) Dopo la cessazione del rapporto di lavoro dell'utilizzatore, i contenuti della casella di posta elettronica sono conservati per ulteriori 30 giorni (senza considerare le tempistiche di *Retention* del sistema di backup) ai soli fini di tutela dei diritti in sede giudiziaria e senza alcuna possibilità di accesso.
36) In nessun caso è possibile richiedere copia delle e-mail inviate o ricevute poiché relative al patrimonio informativo dell'organizzazione e contenenti comunicazioni esclusivamente legate al rapporto di lavoro.
37) L'utilizzatore del sistema di posta, in caso di sospensione del servizio per ferie o malattia, è tenuto autonomamente all'impostazione del messaggio di risposta automatica delle e-mail e alla richiesta di inoltro ai colleghi oppure al diretto superiore.
38) In caso di assenza dell'utilizzatore intestatario dell'*account* e-mail e in presenza di specifiche necessità istituzionali di accesso ai messaggi di posta, il diretto superiore può richiedere ai Sistemi Informativi l'accesso al singolo messaggio o all'intera cartella, il *forward* momentaneo o definitivo dell'*account* di posta su altro indirizzo. Di tale attività deve essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile.
39) Nel caso si riceva una e-mail visibilmente contraffatta da un collega, è necessario informare immediatamente il supporto tecnico.
40) Nel caso la marcatura come messaggio indesiderato di un insieme ricorrente di messaggi di spam non riduca il problema, sono attivabili i cosiddetti filtri personalizzati, in grado di marcare automaticamente tipologie di e-mail indesiderate; nella Intranet sono disponibili le istruzioni per l'attivazione della specifica funzionalità.
41) Al fine di contenere lo spazio di memoria del server di posta, in conformità ai principi di minimizzazione dei dati (art. 5, par. 1, lett. c GDPR) e di limitazione della conservazione (art. 5, par.

1, lett. e) GDPR) l'utilizzatore del servizio di posta elettronica provvede alla periodica cancellazione delle e-mail non rilevanti per la propria all'attività lavorativa.

42) Nel caso di comportamenti anomali del personal computer, evidenziati a seguito dell'apertura di una e-mail, di un click su un link o di un download di un file, è necessario:
    a. staccare immediatamente il cavo di rete;
    b. lasciare il computer acceso;
    c. segnalare immediatamente l'accaduto ai Sistemi Informativi e al proprio Dirigente.
43) I documenti che generano, o fanno parte di processi che hanno valenza amministrativa nonché quelli aventi efficacia esterna rispetto all'organizzazione (come determine, delibere, decreti, verbali, circolari e contratti), in quanto documenti di preminente carattere giuridico-probatorio e fondamentali per la gestione dei procedimenti amministrativi, possono essere inviati via posta elettronica soltanto dopo essere stati oggetto di registrazione di protocollo.
44) I sistemi di posta elettronica convenzionale non consentono di assicurare le dovute caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità prescritte dalla disciplina di settore applicabile alla conservazione digitale. Per tale motivazione la conservazione dei documenti necessari per l'ordinario svolgimento e la continuità delle attività deve essere assicurata utilizzando gli specifici sistemi di gestione documentale, individuando i documenti che nel corso dell'attività lavorativa devono essere via via archiviati con modalità idonee a garantire tali caratteristiche.

UTILIZZO DEI METADATI NELLA GESTIONE DELLA POSTA ELETTRONICA

45) In conformità con i provvedimenti e il documento di indirizzo dell'Autorità Garante per la Protezione dei Dati personali, l'organizzazione effettua trattamenti di metadati relativi ai log di posta elettronica esclusivamente al fine di garantire il corretto funzionamento e la sicurezza del sistema. Dette informazioni sono conservate per un massimo di 90 giorni, così come indicato dal provider del servizio di posta elettronica. Tali informazioni includono dettagli sulle operazioni di invio, ricezione e smistamento dei messaggi, come indirizzi e-mail di mittente e destinatario, indirizzi IP dei server e dei sistemi client coinvolti, orari di invio/ritrasmissione, dimensioni del messaggio, presenza e grandezza di eventuali allegati, e, in alcuni casi, l'oggetto del messaggio.
46) I metadati sono registrati automaticamente dai sistemi, indipendentemente dalla percezione o volontà dell'utente, ma si specifica che restano distinti dal contenuto del messaggio (corpo ed *envelope* del messaggio), che rimane sotto il controllo esclusivo dell'utente e protetto dalle regole di riservatezza della corrispondenza.
47) Il trattamento dei log avviene nel rispetto dei principi di limitazione della finalità, protezione dei dati per impostazione predefinita e progettazione, trasparenza e limitazione della conservazione. Si evidenzia come la raccolta generalizzata avviene comunque nel rispetto delle opportune garanzie legali e sindacali ai sensi dell'art. 4 della Legge 300/1970 (Statuto dei lavoratori).
48) Il trattamento dei metadati, generati dall'impiego di strumenti tecnologici, (ad es., e-mail, archiviazione documentale, etc.) e dei file di log generati dall'utilizzo della rete Internet avviene esclusivamente per le seguenti finalità:
    a. garantire il funzionamento e la sicurezza dei sistemi (ad esempio, prevenire accessi non autorizzati e proteggere i dati da incidenti informatici);
    b. per esigenze organizzative e produttive, nonché per la tutela del patrimonio informativo dell'organizzazione, ai sensi dell'art. 4, comma 1, dello Statuto dei Lavoratori.
49) Il trattamento è svolto senza determinare un'ingerenza ingiustificata nei diritti e le libertà fondamentali degli interessati ed è garantita l'accessibilità selettiva ai metadati da parte del personale espressamente autorizzato e istruito in materia di protezione dei dati e la tracciatura degli accessi effettuati.

Art. 13. - Posta Elettronica Certificata (PEC)

1) La Posta Elettronica Certificata (PEC) è un sistema nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici, ed è garantita la tracciabilità della casella mittente; il circuito è certamente più sicuro della posta elettronica convenzionale ma non è esente da rischi. Per questo motivo valgono le stesse regole e indicazioni fornite per la posta elettronica convenzionale, sia per l'eventuale accesso diretto che tramite piattaforme applicative di gestione documentale.
2) La gestione, l'organizzazione e le modalità d'uso del sistema di Posta Elettronica Certificata (PEC) sono disciplinate all'interno del MANUALE DI GESTIONE DEI FLUSSI DOCUMENTALI.

Art. 14. - Firma elettronica

1) Le Firme Elettroniche, ai sensi del Regolamento (UE) 2014/910 (eIDAS, *Electronic IDentification Authentication and Signature*) e del Codice dell'Amministrazione Digitale possono essere di 4 tipi:

Tipologia Firma	Definizione	Esempi	Valore probatorio
Elettronica semplice [art. 3, comma 10 eIDAS]	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare	Messaggio di posta elettronica ordinaria o una sottoscrizione (scansione firma apposta al documento) che non ha tutti i requisiti delle altre sottoscrizioni elettroniche di livello superiore	Liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità (art.21 del CAD)
Avanzata [art. 3, comma 11 eIDAS] [Requisiti previsti all'art 26 eIDAS]	a) è connessa unicamente al firmatario; b) è idonea a identificare il firmatario; c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo; e d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.	Firma grafometrica utilizzata su tablet in molti contesti tra i quali le banche e le assicurazioni.	Garantisce l'identità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'art. 2702 del Codice civile. L'utilizzo del dispositivo di firma qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria.
Qualificata [art. 3, comma 12 eIDAS]	Firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche	Smart card, Token (sicurezza)	Garantisce l'identità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'art. 2702 del Codice civile. L'utilizzo del dispositivo di firma qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria.
Digitale [art. 24 CAD]	Particolare tipo di firma qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici	Smart card, Token (sicurezza), Firma digitale remota.	Garantisce l'identità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'art. 2702 del Codice civile. L'utilizzo del dispositivo di firma qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria.

2) L'utilizzatore dotato di strumenti di firma è responsabile della conservazione in sicurezza di tutte le componenti (PIN e Password, oppure hardware come la Smart card o il token di firma). La perdita degli strumenti di firma o il semplice sospetto della perdita di segretezza della password o del PIN, deve essere immediatamente comunicata al supporto tecnico dei Sistemi Informativi per l'attivazione delle procedure di disabilitazione, al CISO e al Privacy Officer / DPO.
3) È fondamentale conservare separati i dispositivi di firma (Smart card) dal PIN e dalla password (è preferibile provare a ricordare, senza dover trascrivere le credenziali).
4) La firma di atti o documenti dell'organizzazione è responsabilità diretta dell'intestatario della firma elettronica (di qualsiasi tipologia sopra riportata). È vietato firmare per conto di altri soggetti anche nel caso di autorizzazione verbale o scritta; sono escluse dal divieto le sole firme cosiddette automatiche (ad es., attraverso il sistema SDI).
5) I documenti firmati digitalmente, per definizione, non sono ripudiabili a meno di querela di parte.
6) È possibile firmare atti o documenti dell'organizzazione solo se in formato PDF, PDF/A (progettato per la conservazione dei documenti amministrativi) o XML. Gli altri formati sono vietati, a meno di specifica autorizzazione o descrizione nel Manuale di gestione documentale.
7) Le tipologie di firme accettate sono P7M (CAeDES), PDF (PAeDES) e XML (XAeDES). Altri formati non sono accettati dall'organizzazione o dalle piattaforme di conservazione.
8) Il rinnovo dei certificati di prossima scadenza è in carico al fornitore del servizio di firma. L'aggiornamento dei certificati del software di verifica delle firme è a carico del singolo utilizzatore; è necessario contattare il supporto tecnico dei Sistemi Informativi nel caso di problemi.
9) Le regole per la sicurezza delle password riportate all'Art. 11 - Corretto uso delle Credenziali di autenticazione del presente Regolamento sono valide anche nella definizione della password e PIN/PUK di firma.
10) Nel caso il software di verifica delle firme segnali delle anomalie è necessario:
    a. Verificare che la lista delle *Certification Authority* (CA) sia aggiornata;
    b. Verificare il firmatario;
    c. Richiedere di nuovamente il documento firmato al firmatario.
11) La conservazione sostitutiva dei documenti firmati digitalmente segue quanto previsto dalla regolamentazione in materia. Si faccia riferimento alla specifica documentazione a cura del Responsabile della conservazione.

Art. 15. - Instant messaging

1) Gli strumenti di comunicazione sincrona permettono facili e immediati scambi di messaggi di servizio tra colleghi; permettono anche la condivisione dei documenti, delle immagini e dei video senza richiedere particolari prerequisiti, a meno della copertura Internet o Wi-Fi e l'utilizzo di un dispositivo *mobile*. I prodotti più diffusi sono WeChat, Facebook Messenger e WhatsApp. L'utilizzo di questi strumenti in ambito lavorativo è tollerato per le sole comunicazioni interpersonali di servizio (appuntamenti, segnalazioni, ecc.).
2) La condivisione di dati personali o di informazioni riservate relative all'ambito lavorativo su piattaforme di messaggistica gratuite è vietato per le seguenti motivazioni:
    a. I dati sono inviati (inconsapevolmente) a server posizionati in paesi extra UE, senza le dovute prescrizioni previste al Capo V del GDPR, artt. 44-50 in termini di regolamentazione, protezione e garanzie per gli interessati;
    b. Tutte le informazioni (testo, immagini e video) sono indicizzate per denominazione e contenuti;
    c. Tutti gli utenti sono profilati, anche se non appartenenti allo specifico ambito o sconosciuti al sistema (ad es., foto di gruppo);
    d. Non è al momento prevedibile quale utilizzo potrà essere fatto in futuro dei dati inviati, né quali potranno essere gli impatti sugli interessati;

e. Le impostazioni di sicurezza di default dei dispositivi *mobile* non garantiscono generalmente un adeguato livello di sicurezza e protezione dei dati.

3) Eventuali messaggi arrivati su dispositivi *mobile* contenenti dati personali o informazioni riservate legate all'ambito lavorativo devono essere cancellate.
4) Le app per *mobile* possono essere scaricate soltanto dagli *store* ufficiali. In caso di dubbi sugli strumenti in uso dell'organizzazione contattare il supporto tecnico.
5) Verificare periodicamente le impostazioni relative alle autorizzazioni delle applicazioni dei dispositivi *mobile* e le relative impostazioni sulla privacy al fine di limitare eventuali accessi ai contenuti.
6) Per i sistemi di messaggistica istantanea valgono le stesse considerazioni di sicurezza esposte nei commi relativi alla posta elettronica, in particolare per quanto riguarda mittenti, contenuti, link e allegati.

Art. 16. - Sistemi informatici

1) I sistemi informatici sono installati presso le singole postazioni di lavoro (client) o presso i datacenter (server) soltanto dopo:
    a. Aggiornamento di tutte le componenti software (firmware, sistema operativo, middleware e componenti, applicazioni e piattaforme software);
    b. Installazione delle componenti obbligatorie (come agent e antivirus);
    c. Verifica tramite procedura di *vulnerability assessment* senza evidenze rispetto ad elementi elevati ("**HIGH**") o critici ("**WARNING**");
    d. Redazione della necessaria documentazione sul sistema e sulle eventuali modalità di re-installazione e ripristino;
    e. Aver testato le funzionalità di base ed aver redatto il documento di omologazione (*check-list*).
2) La lista dei requisiti minimi previsti per il collegamento alla rete dell'organizzazione è redatta e mantenuta aggiornata alle migliori pratiche di settore a cura dei Sistemi Informativi.
3) Il collegamento di sistemi o dispositivi non conformi a tali requisiti minimi, ad esempio per vincoli tecnici o di compatibilità, può avvenire in via esclusiva su specifica sottorete, separata e posta in sicurezza rispetto alla rete dell'organizzazione.
4) I sistemi informativi provvedono all'aggiornamento dell'inventario degli asset con specifico riferimento ai sistemi informativi e di rete rilevanti per l'erogazione dei servizi.

Art. 17. - Applicazioni software

1) Le applicazioni software, specie se di tipo web, sviluppate da terze parti possono essere installate presso il datacenter, locale o in cloud dell'organizzazione esclusivamente dopo avvenuto penetration test (ad es., basato su OWASP Top 10) con esito positivo. Nel caso di applicazioni SaaS qualificate AgID e pubblicate nel relativo Marketplace non è necessario procedere con i test poiché già ampiamente effettuati in fase di pre-qualificazione.
2) Sono escluse dall'obbligo di penetration test le applicazioni o le piattaforme standard.
3) Eventuali ulteriori requisiti potranno essere richiesti da parte dei Sistemi Informativi in funzione delle specificità dell'applicazione in questione.

Art. 18. - Dispositivi Mobili (smartphone, tablet e *pen drive*/*portable disk*)

1) L'uso personale dei dispositivi mobili forniti dall'organizzazione è tollerato a patto che non siano salvati nel sistema dati estranei all'attività lavorativa, specie se di tipo personale. Eventuali documenti contenenti dati personali devono essere rimossi immediatamente.
2) È vietata l'installazione di applicazioni non direttamente distribuite, autorizzate e presenti nella *white list* dell'organizzazione, anche se provenienti dagli *store* ufficiali.

3) I dispositivi *mobile* forniti dall'organizzazione hanno impostazioni di sicurezza predefinite, conformi alla normativa vigente e alle politiche di sicurezza dell'organizzazione. È vietato modificare le impostazioni di sicurezza anche se al fine di permettere il funzionamento di applicazioni software; eventuali *workaround* dovranno essere specificatamente omologati dai Sistemi Informativi dell'organizzazione; è necessario contattare il supporto tecnico in caso di problemi.
4) Nell'ipotesi di smarrimento o furto di un dispositivo fornito dall'organizzazione, contenente dati personali riconducibili all'organizzazione titolare del trattamento dei dati, l'utilizzatore è tenuto a comunicare l'accaduto al CISO e al Privacy Officer / DPO per l'attivazione della procedura di data *breach* e/o incidente alla sicurezza e, a seguire, ai Sistemi Informativi dell'organizzazione per l'attivazione delle previste procedure di sicurezza (*device wipe-out*).
5) Il trasporto al di fuori del perimetro dell'organizzazione di dispositivi di memorizzazione di proprietà dell'organizzazione contenenti dati sensibili è vietato. La responsabilità in caso di perdita, smarrimento e involontaria diffusione dei dati contenuti nel dispositivo durante il trasporto al di fuori del perimetro dell'organizzazione, sarà attribuita all'utilizzatore assegnatario.
6) Il Dirigente della UO può autorizzare l'utilizzo dei dispositivi di memorizzazione a patto che siano implementati idonei strumenti di criptazione, in linea con gli standard di sicurezza internazionale (ad esempio, almeno di tipo AES-256), in modalità nativa a livello di dispositivo o per singola cartella/file.
7) In tutti i casi di trasporto dei dati al di fuori del perimetro della rete dell'organizzazione è tassativamente prevista la criptazione dei contenuti, anche nel caso di pseudonimizzazione.
8) I dati possono essere conservati per il tempo necessario al raggiungimento della finalità prevista, secondo quanto riportato dal massimario di conservazione; a conclusione dell'attività di trattamento, raggiunta la finalità, i file devono essere completamente cancellati.
9) I commi precedenti non si applicano ai dati totalmente anonimizzati.
10) Alla conclusione del rapporto di lavoro l'utilizzatore è tenuto a riconsegnare il dispositivo o sistema inizialmente assegnato, segnalando al personale tecnico eventuali problematiche emerse durante l'utilizzo. Dopo un massimo di 30 giorni il sistema o il dispositivo sono sottoposti a procedura di cancellazione completa (*wipe-out*), senza alcuna possibilità di ripristino.

Art. 19. - Dispositivi di proprietà personale (*bring-your-own-device policy* - BYOD)

1) I dispositivi di proprietà personale possono essere utilizzati soltanto come sistemi isolati non collegati alla rete dell'organizzazione, a meno del Wi-Fi con accesso di tipo *guest* (ove presente). I sistemi di monitoraggio effettuano controlli automatici continui e segnalano al personale tecnico eventuali sistemi e dispositivi non catalogati e non autorizzati che abbiano effettuato un collegamento diretto alla rete locale dell'organizzazione (LAN). Eventuali sistemi o dispositivi non autorizzati collegati alla rete dell'organizzazione potrebbero essere bloccati e l'azione sarà considerata attacco al sistema informatico.
2) È severamente vietato il collegamento alla rete dell'organizzazione di sistemi o dispositivi non distribuiti ufficialmente dai Sistemi Informativi. Il personale che effettuerà il collegamento diretto alla rete dell'organizzazione (sono escluse i Wi-Fi pubblici) sarà soggetto a sanzioni disciplinari. Saranno inoltre addebitati all'utilizzatore eventuali costi di rispristino o ulteriori danni che dovessero originarsi da un collegamento non autorizzato. Rientrano nei dispositivi del presente comma modem, router, switch, dispositivi wireless, Bluetooth o qualsiasi altro dispositivo che possa in qualche modo ampliare la superficie di esposizione e quindi i rischi connessi.
3) Il collegamento alla rete Wi-Fi pubblica dell'organizzazione (ove disponibile) dei dispositivi di proprietà personale come laptop, tablet o smartphone è possibile seguendo la specifica procedura di autorizzazione, registrazione e autenticazione. In tutti i casi è prevista la registrazione delle attività dell'utilizzatore e la navigazione Internet, conformemente a quanto previsto all'art. 20 - Navigazione Internet.

4) In conformità alla normativa vigente in tema di misure di protezione da adottare nelle attività di trattamento e considerata la non appartenenza di questa tipologia di dispositivi al perimetro di sicurezza dell'organizzazione, è vietato salvare dati personali raccolti durante le attività lavorative o comunque riferibili all'organizzazione sui dispositivi di proprietà personale, specialmente nel caso di dati di natura particolare.
5) Al fine di garantire un adeguato livello di sicurezza nell'utilizzo dei dispositivi di proprietà personale, anche per la sola consultazione delle piattaforme pubbliche (ad es., posta elettronica), comunque equiparabile a quanto stabilito per l'organizzazione, è necessario che i tali dispositivi siano dotati almeno di antivirus con basi aggiornate, firewall locale attivo, aggiornamento del sistema operativo e dei componenti, totale assenza di software copiato o "*crackato*".
6) In nessun caso è possibile installare sui dispositivi di proprietà personale i software con licenza di proprietà dell'organizzazione.
7) Il trasporto al di fuori del perimetro dell'organizzazione di dispositivi di memorizzazione personali contenenti dati sensibili afferenti all'organizzazione è vietato. Eventuali repliche o copie di sicurezza delle informazioni devono essere autorizzate e tracciate, secondo le procedure previste. La responsabilità in caso di perdita, smarrimento e involontaria diffusione dei dati contenuti nel dispositivo durante il trasporto al di fuori degli uffici, sarà attribuita all'utente titolare registrato.
8) Nell'ipotesi di smarrimento o furto di un dispositivo di proprietà personale contenente dati personali riconducibili all'organizzazione titolare del trattamento dei dati, è obbligatorio comunicare l'accaduto al CISO e al Privacy Officer / DPO per l'attivazione della procedura di *Data Breach* e incidente alla sicurezza.

Art. 20. - Navigazione Internet

1) La rete Internet è la fonte di informazioni e documentazione più vasta esistente, quindi irrinunciabile tanto per il personale operativo quanto per il personale amministrativo. L'organizzazione mette a disposizione questo servizio a patto che se ne faccia buon uso ovvero che le finalità di navigazione siano connesse esclusivamente all'attività lavorativa.
2) A meno di specifica autorizzazione del proprio Dirigente comunicata al Responsabile dei Sistemi Informativi, è vietato navigare in tutti i siti web appartenenti alle categorie previste nell'Appendice *Content Filtering Rating Categories,* sia dalla rete locale che Wi-Fi, navigare per fini ludici o personali, effettuare *upload* o *download* di file e documenti non connessi all'attività lavorativa, effettuare *streaming* audio o video (es. radio o tv via Internet), effettuare chat on-line se non specificatamente autorizzati e comunque limitate a finalità lavorative.
3) È tassativamente vietata la navigazione in siti Internet palesemente incompatibili con le finalità dell'organizzazione, che istighino a comportamenti illegali, che consentano o siano a rischio di diffusione di virus, cavalli di Troia o di altri programmi il cui obiettivo sia la distruzione, alterazione, sabotaggio, intercettazione, *hacking* o pirateria informatica a danno dei computer di altri utenti interni o esterni al perimetro dell'organizzazione.
4) È inoltre vietato navigare in siti web che possano comportare nei sistemi deputati al monitoraggio e alla protezione della connessione Internet, trattamenti involontari di dati personali di tipo sensibile riconducibili agli utilizzatori del servizio (esempio convinzioni religiose, politiche, stato di salute, vita sessuale).
5) La navigazione web non è esente da rischi, nonostante siano già attivi diversi strumenti di protezione; gli impatti potrebbero non essere legati al singolo computer ma interessare parte o addirittura l'intero patrimonio informativo dell'organizzazione, con risvolti imprevedibili sulla continuità stessa dei servizi e danni reputazionali e di immagine. Per queste motivazioni è sempre in capo al singolo utilizzatore la verifica di:
    a. **Indirizzo del sito web**: è necessario verificare più di una volta l'indirizzo completo (attenzione ai siti web che appaiono simili ma non lo sono: www.comune.senigallia.com o

www. senigallia.<*sitowebstrano*>.it; *Attenzione*: la dimensione del font della barra dell'indirizzo del browser non aiuta);

b. **Certificato**: evitare i siti web non sicuri (con protocollo "http") e nel caso di siti web con protocollo "https" fare attenzione alla perfetta corrispondenza del certificato con intestazione e indirizzo del sito web in questione;
c. **Riferimenti**: i siti web dei cosiddetti *scammer* o truffaldini non riportano né l'indirizzo della sede né tantomeno numeri telefonici o altri riferimenti dell'organizzazione (in Italia è obbligatoria la pubblicazione della partita IVA delle organizzazioni registrate all'Agenzie delle Entrate);
d. **Link**: i link devono essere verificati prima di essere lanciati anche nel caso appaiano a prima vista del tutto familiari (soprattutto nell'aspetto grafico); questo al fine di evitare attacchi di tipo *phishing*; la verifica può essere effettuata posizionando il cursore del mouse sul link in modo da visualizzare la destinazione reale (ad esempio evitare di fare click su link del tipo https://www.regione.marche.it nel caso vi sia un rimando ad altro sito, ad esempio: www.<altrositowebstrano>.it);
e. **Download**: evitare di scaricare da siti web non ufficiali qualsiasi documento, software applicativo, driver o componente aggiuntivo (*plug-in* del browser o componenti "dinamici" come ActiveX o funzioni JavaScript), includendo anche le app per dispositivi *mobile*;
f. **Contenuti**: verificare la presenza di errori sintattici grossolani (dovuti a traduzione automatiche o a profilazione all'utenza meno attenta) al fine di riconoscere siti web non ufficiali (tecnicamente denominati *fake*);
g. **Verifiche web**: attraverso i motori di ricerca è possibile trovare altre informazioni sul singolo sito web che possono aiutare nell'identificazione; provare ad effettuare una ricerca in un motore generalista con la denominazione del sito web seguita dalle parole "opinioni" o "recensioni" (ricerca: <altrositowebstrano>.it opinioni).

Nei casi dubbi non aprire il sito web, interrompere la navigazione, chiudere il browser e, nel caso il sistema inizi ad avere comportamenti singolari, disconnettere il sistema dalla rete locale (senza spegnere) e contattare immediatamente il supporto tecnico che provvederà ad effettuare le verifiche secondo le procedure di sicurezza.

6) L'utilizzo moderato e sporadico degli strumenti informatici dell'organizzazione per finalità private è tollerato, solo nel caso che questo non comporti nocumento all'attività lavorativa.
7) I rischi derivanti dall'utilizzo delle informazioni personali (ad es. numeri di carte di credito) durante la navigazione web estranea alle attività lavorative, sono sempre in capo all'utilizzatore. Il Titolare non potrà essere ritenuto responsabile di eventuali danni dovuti a perdite di riservatezza, integrità o disponibilità di dati personali inviati in sessioni effettuate con strumenti dell'organizzazione.
8) L'acquisizione, conservazione, trasmissione o diffusione di file dal contenuto illegale, discriminatorio per origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, stato di salute o disabilità, genere, colore dei capelli, età, vita sessuale o orientamento sessuale della persona è vietato. Eventuali abusi o contenuti illegali che si dovessero evidenziare durante la navigazione devono essere comunicati al supporto tecnico per le valutazioni del caso.
9) L'acquisizione, conservazione, trasmissione o diffusione di materiale che violi il diritto d'autore, i marchi, i segreti commerciali o i diritti di brevetto di qualsiasi persona o organizzazione è vietato. Tutti i materiali pubblicati su Internet sono protetti da copyright e/o brevettati, salvo diversa indicazione[6] (Legge 633/1941 – "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio).

[6] Ad esempio, le 6 licenze di tipo Creative Commons, definite dalla combinazione di quattro attributi che permettono di stabilire esplicitamente quali siano i diritti riservati, modificando la regola di default in cui tutti i diritti sono riservati.

10) La trasmissione di informazioni proprietarie, riservate o altrimenti sensibili, contenenti dati personali di tipo particolare è vietata. Solo se specificatamente autorizzato, l'utente può effettuare l'invio/*upload* a condizione di adottare controlli specifici e livelli di protezione elevati forniti dalla criptazione (cosiddetta *in-transit,* tramite protocolli criptati ovvero *https*, *ftps*, etc.).
11) La larghezza di banda della rete locale (interna) dell'organizzazione come anche la connettività Internet è una risorsa condivisa e limitata. Considerato che gli utilizzi indebiti di un singolo utilizzatore potrebbero impattare sulle attività degli altri, sono adottate delle politiche di gestione della banda in funzione delle tipologie di attività svolte; tale modalità di funzionamento garantisce il massimo delle prestazioni possibili in funzione delle priorità assegnate (*packet shaping*).
12) Le attività di navigazione internet degli utilizzatori sono monitorate da un sistema automatico che verifica i seguenti parametri:
    a. Quantità di dati scaricati giornalmente e mensilmente ;
    b. Tipologie di siti web visitati (in visione aggregata e conformi alle politiche di *content filtering*);
    c. Tempistiche totali di navigazione Internet.

    Eventuali comportamenti degli utilizzatori anomali, non conformi o superiori ai parametri generali sopra riportati, quindi non funzionali al corretto funzionamento del servizio, potranno comportare la disattivazione automatica dell'*account* di accesso per motivi di sicurezza, anche al fine di garantire la necessaria continuità operativa.
13) In conformità alla normativa sulla sicurezza IT e protezione dei dati personali, perseguendo i principi generali ovvero necessità, correttezza, pertinenza e non eccedenza, è garantita la sovra-registrazione dei dati del traffico Internet dell'utilizzatore, la cui conservazione non sia necessaria (è attivata la cd. rotazione dei file di log).
14) La conservazione dei file di registrazione della navigazione degli utilizzatori è limitata al massimo a 21 giorni, che è considerato il periodo strettamente necessario per il perseguimento delle finalità organizzative, produttive e di sicurezza dell'organizzazione, fatti salvi in ogni caso specifici obblighi di legge. Sono esclusi dalle regole di conservazione i dati aggregati di navigazione che possono essere conservati più a lungo per le sole finalità statistiche e di governo.

Art. 21. - Utilizzo del personal computer (desktop) o del portatile (laptop)

1) La continuità dei servizi è strettamente legata alla normale operatività di tutti i dispositivi della catena tecnologica, a partire dalla postazione di lavoro fino al network. Utilizzi impropri dei dispositivi e delle apparecchiature possono produrre effetti indesiderati e potenzialmente compromettere il funzionamento di altri sistemi che, in casi particolari, potrebbe causare anche danni alle persone. L'utilizzatore di sistemi e servizi IT sarà ritenuto responsabile per i costi di riparazione nel caso il danno sia causato da un uso improprio o da negligenza.
2) È vietato modificare la posizione, la configurazione hardware e software, la modalità di collegamento alla rete dell'organizzazione e all'alimentazione elettrica, da parte dell'utilizzatore o di personale esterno, senza specifica autorizzazione del personale del servizio di supporto tecnico [è necessario seguire specifica procedura].
3) Non è consentito l'uso o l'installazione di software applicativi diversi da quelli distribuiti ufficialmente dai Sistemi Informativi (ai sensi del D.lgs. n. 518/1992 sulla tutela giuridica del software e Legge n. 248/2000 nuove norme di tutela del diritto d'autore), inclusi nel catalogo dei servizi e nella *white list del software.* Sono periodicamente effettuati controlli e, in caso di presenza di componenti o applicazioni non autorizzate, il personale dei Sistemi Informativi procede con la disinstallazione, anche in modalità "trasparente".
4) È vietato conservare nei sistemi e unità di memorizzazione assegnati, file, documenti, e-mail, immagini, video non legati alle finalità lavorative e professionali, in particolar modo se di contenuto osceno o violento, offensivo alla morale o alla pubblica decenza, oltraggioso e/o discriminatorio.

5) Il trasporto al di fuori del perimetro dell'organizzazione di dispositivi di memorizzazione contenenti dati personali e sensibili è vietato. Eventuali repliche o copie di sicurezza delle informazioni devono essere autorizzate e tracciate, secondo le procedure previste. La responsabilità in caso di perdita, smarrimento e involontaria diffusione dei dati contenuti nel dispositivo durante il trasporto al di fuori degli uffici, sarà attribuita all'utente titolare registrato.
6) L'utilizzatore di sistemi e servizi IT è invitato alla immediata segnalazione al servizio di supporto tecnico di eventuali danni, perdita di funzionalità parziale o totale, riduzione delle performance complessive dei dispositivi o delle apparecchiature informatiche.
7) Nel caso di malfunzionamenti o comportamenti inusuali dei sistemi, configurabili come compromissioni, l'utilizzatore è tenuto a:
    a. scollegare immediatamente il sistema dalla rete locale, lasciando il sistema acceso;
    b. segnalare l'accaduto al proprio superiore;
    c. aprire una richiesta di intervento (ticket) ai Sistemi Informativi.
8) Eventuali specifiche indicazioni o istruzioni fornite dal personale di supporto tecnico devono essere rispettate al fine di garantire il miglior funzionamento possibile dei sistemi, dei dispositivi, dei servizi e delle risorse condivise.
9) Concluse le attività lavorative o nel caso di momentanea assenza o allontanamento dalla postazione di lavoro, l'utilizzatore di sistemi e servizi IT è tenuto alla disconnessione dei servizi e degli applicativi attivi o alla completa disconnessione/arresto del sistema (Windows-l (elle), blocco dell'utilizzatore connesso oppure Start – Arresta / Disconnetti).
10) Gli utilizzatori sono tenuti a spegnere i personal computer o i dispositivi assegnati o in uso alla conclusione della sessione di lavoro, a meno di specifiche e contingenti necessità di successivi collegamenti da remoto.
11) Il desktop come le cartelle di rete, al pari della scrivania fisica, devono essere mantenuti in ordine (cd. *clean desktop policy*) in modo da facilitare successive ricerche.

Art. 22. - Sistemi e dispositivi di acquisizione e stampa

1) L'organizzazione prevede l'utilizzo di sistemi e dispositivi di acquisizione e stampa dei documenti. La vigente normativa in tema di digitalizzazione prevede però l'acquisizione nativa dei documenti digitali, la loro comunicazione, elaborazione sempre in formato digitale e, infine, la conservazione sostitutiva, sempre digitale[7]. In attesa di completare il processo di digitalizzazione dei documenti e, parallelamente, la revisione dei processi amministrativi, è possibile stampare esclusivamente la documentazione strettamente necessaria, avendo cura di ritirarla immediatamente dal dispositivo o sistema di stampa condiviso, in modo da evitare la potenziale diffusione di informazioni, anche di tipo riservato.
2) In ogni caso è vietata la stampa o acquisizione di documenti personali dell'utilizzatore, estranei all'attività lavorativa svolta.
3) A meno di impossibilità tecnica o amministrativa, i documenti dovrebbero essere sempre stampati in modalità fronte-retro.
4) La carta deve essere caricata negli appositi alloggiamenti evitando piegature o caricamenti parziali, avendo cura di sfogliare leggermente, e senza disallineamenti dei bordi, al fine di evitare inceppamenti.
5) In ogni caso l'utilizzatore non è autorizzato a smontare il dispositivo di stampa anche nel caso di inceppamenti della carta che dovranno essere gestiti tramite segnalazione ai sistemi informativi o al riferimento tecnico del dispositivo stesso.

[7] Decreto della Presidenza del Consiglio del 13 novembre 2014, che all'articolo 17 comma 2

Art. 23. - Utilizzo dei telefoni fissi in dotazione

1) Il telefono fisso, analogico o digitale, in dotazione agli utilizzatori è uno strumento di lavoro, utilizzabile esclusivamente per ricevere ed effettuare comunicazioni di servizio. Sono esclusi impieghi a carattere personale, comunque non strettamente inerenti all'attività lavorativa. Sono permesse esclusivamente telefonate di carattere personale per i soli motivi di comprovata necessità, urgenza ed emergenza.
2) L'utilizzatore dei telefoni fissi è informato sulla necessità dell'organizzazione di registrare le telefonate in ingresso o uscita, rispetto alle sole seguenti informazioni:
    a. Data e orario della chiamata (ingresso o uscita);
    b. Numero chiamato o chiamante;
    c. Durata in minuti della telefonata;
    d. Eventuali costi addebitati all'organizzazione.

   Le registrazioni sono effettuate e utilizzabili nei limiti previsti dallo Statuto dei lavoratori con particolare riguardo al controllo a distanza del lavoratore (art. 4 L. 300/70), del Codice Privacy e del Regolamento (UE) 2016/679 e sono conservate per un periodo non superiore a 3 mesi (tempo tecnico per eventuale verifica sulla contabilizzazione di costi extra contratto da parte del fornitore del servizio di fonia).
3) In specifici ambiti operativi connessi alla gestione delle emergenze e alla sicurezza dei servizi (a titolo esemplificativo: centralini della Polizia Locale, Protezione Civile o analoghi servizi di pronto intervento in caso di emergenza) è prevista la registrazione audio delle chiamate in ingresso. Tali registrazioni sono effettuate esclusivamente per finalità di tutela degli operatori, degli utenti e per esigenze di sicurezza e gestione delle emergenze, nel rispetto della normativa vigente in materia di protezione dei dati personali e dell'art. 4 della Legge 300/1970. Gli interessati sono previamente informati mediante idonea informativa e, ove necessario, mediante messaggi automatici all'avvio della chiamata. Il periodo di conservazione è limitato a quanto strettamente necessario e proporzionato alle finalità perseguite e comunque non superiore a 6 mesi, fatti salvi eventuali obblighi di legge, esigenze di sicurezza o necessità di tutela dei diritti dell'Ente.
4) Gli utenti sono autorizzati alle chiamate nazionali, di numeri fissi e mobili. Le chiamate a numeri europei o internazionali sono bloccate a meno di specifica autorizzazione.

Art. 24. - Utilizzo degli smartphone, tablet e SIM dell'organizzazione

1) Gli smartphone, tablet e SIM dell'organizzazione sono strumenti di lavoro, impiegabili esclusivamente per ricevere ed effettuare comunicazioni di servizio. Sono esclusi impieghi a carattere personale, comunque non strettamente inerenti all'attività lavorativa. Sono permesse esclusivamente telefonate di carattere personale per i soli motivi di comprovata necessità, urgenza ed emergenza.
2) In generale si applicano le stesse prescrizioni previste per la telefonia fissa riportate nel precedente articolo.
3) L'utilizzatore è tenuto a comunicare immediatamente l'eventuale perdita, smarrimento, furto del dispositivo o SIM in dotazione, al fine di provvedere al blocco e denuncia alle Autorità competenti.

Art. 25. - Gestione dei documenti e degli spazi di archiviazione digitali

1) Gli spazi di archiviazione e condivisione dei documenti dell'organizzazione sono basati su piattaforma Microsoft 365, tramite SharePoint Online e OneDrive, e si articolano nelle seguenti tipologie:

   a. Spazio personale dell'utente (OneDrive)

Destinato alla conservazione dei documenti personali di lavoro, in corso di elaborazione o non ancora destinati alla condivisione. Lo spazio è associato nominalmente all'utente ed è accessibile esclusivamente dal medesimo, salvo i casi previsti dal presente regolamento.

b. Siti SharePoint di Unità Operativa

Utilizzati per la condivisione dei documenti tra gli utilizzatori appartenenti alla medesima Unità Operativa / ufficio. I documenti sono organizzati in raccolte documentali (Document Library) strutturate secondo le esigenze operative del servizio.

c. Siti SharePoint di Progetto

Destinati alla collaborazione tra più Unità Operative per attività trasversali, progetti o gruppi di lavoro.

L'accesso è consentito esclusivamente agli utenti espressamente autorizzati.

d. Raccolte documentali per Scansioni

Spazi SharePoint dedicati alla memorizzazione temporanea dei documenti digitalizzati tramite dispositivi multifunzione. I file devono essere successivamente archiviati nelle corrette raccolte documentali di competenza o eliminati.

e. Condivisione controllata via web

La condivisione di documenti con altri utenti interni o, se autorizzato, esterni all'organizzazione avviene esclusivamente tramite le funzionalità di condivisione di SharePoint e OneDrive, nel rispetto delle politiche di sicurezza vigenti.

2) La politica di sicurezza dell'organizzazione non prevede la conservazione di documenti sui dischi locali dei personal computer.
3) I file salvati localmente non sono oggetto di backup e, in caso di guasti o malfunzionamenti, possono andare irrimediabilmente persi. Tutti i documenti di lavoro devono pertanto essere archiviati esclusivamente su SharePoint o OneDrive.
4) All'interno dei siti SharePoint è possibile definire livelli differenziati di autorizzazione, quali, a titolo esemplificativo:
   accesso in sola lettura;
   accesso in modifica;
   accesso limitato a specifiche raccolte documentali.
5) La gestione dei permessi avviene secondo il principio del minimo privilegio necessario ed è di competenza dei Sistemi Informativi o dei referenti autorizzati.
6) I dati archiviati su SharePoint Online e OneDrive sono protetti da sistemi di replica e backup automatico della piattaforma Microsoft 365.
7) È garantita una retention standard, che consente il recupero dei file eliminati o delle versioni precedenti entro i limiti temporali definiti dalle politiche dell'organizzazione (generalmente non inferiori a due settimane), salvo diverse disposizioni normative o tecniche.
8) È vietato conservare su SharePoint, OneDrive o su qualsiasi altro sistema di archiviazione dell'organizzazione file protetti dal diritto d'autore, qualora non espressamente autorizzati o necessari allo svolgimento delle attività istituzionali.
9) Documenti contenenti marchi, segreti commerciali, informazioni riservate o diritti di brevetto devono essere gestiti con particolari accorgimenti di sicurezza e con accesso strettamente riservato. Per tali esigenze è obbligatorio coinvolgere preventivamente i Sistemi Informativi, al fine di definire le corrette modalità di archiviazione e protezione.

10) Gli utilizzatori sono tenuti a:

    a. utilizzare in modo responsabile lo spazio di archiviazione assegnato, rispettando le quote previste per OneDrive e SharePoint;

    b. eliminare periodicamente i documenti non più necessari o duplicati (es. versioni multiple dello stesso file);

    c. evitare la duplicazione di informazioni già presenti in applicativi istituzionali dell'organizzazione (esportazioni non necessarie di dati verso file Excel, Access o analoghi).

11) In caso di assenza dell'utente titolare dello spazio personale (OneDrive) e in presenza di comprovate esigenze istituzionali, il diretto superiore può richiedere ai Sistemi Informativi l'accesso a specifici documenti o all'intero spazio dell'utente. L'operazione deve essere formalizzata mediante apposito verbale, e il lavoratore interessato deve esserne informato alla prima occasione utile, nel rispetto della normativa vigente.
12) I documenti digitali di particolare dimensione in termini di occupazioni di spazio disco, come immagini, progetti, video, sono archiviati in appositi File Server Locale/in Cloud ed accessibili attraverso cartelle di rete condivise esclusivamente con i personale autorizzato all'accesso/gestione.

Art. 26. - File hosting

1) È vietato il caricamento, l'archiviazione o la condivisione di dati personali, dati riservati o comunque riconducibili all'Ente su sistemi di file hosting, piattaforme cloud o servizi di trasferimento file non messi a disposizione o non autorizzati dall'Ente, quali a titolo esemplificativo Google Drive, Dropbox, WeTransfer o servizi analoghi.
2) La condivisione dei documenti informatici deve avvenire esclusivamente tramite i canali e gli strumenti istituzionali, in coerenza con quanto previsto dal Manuale di gestione documentale e, in particolare:

    a. tramite il sistema di posta elettronica istituzionale, ordinaria o certificata, integrato con il sistema di protocollo informatico;

    b. tramite i sistemi ufficiali di condivisione documentale adottati dall'Ente, quali OneDrive e Ropobox, utilizzati secondo le procedure operative previste dal Manuale di gestione documenti e dalle circolari ufficiali interne.
3) L'utilizzo di sistemi di condivisione documentale (es. OneDrive) per l'interscambio di documentazione di dimensioni rilevanti o per specifiche esigenze operative è ammesso esclusivamente nell'ambito delle procedure formalizzate nel Manuale di gestione, che prevedono:
    a. il preventivo invio di un documento riepilogativo tramite posta elettronica istituzionale;
    b. la condivisione dei file tramite cartelle dedicate e temporanee;
    c. la successiva protocollazione unitaria della documentazione;
    d. la revoca degli accessi alla cartella di condivisione al termine del procedimento.
4) Eventuali utilizzi di ulteriori sistemi cloud o di piattaforme di condivisione non già disciplinati nel Manuale di gestione devono essere preventivamente autorizzati dal responsabile competente e comunicati ai Sistemi Informativi, che ne valutano la conformità in materia di sicurezza, protezione dei dati personali e rispetto della normativa vigente.

Art. 27. - *Cloud computing* e servizi IT esterni

1) L'acquisizione di servizi basati su tecnologia cloud come IaaS, PaaS e SaaS deve essere conforme alla normativa nazionale e alle Politiche di approvvigionamento dell'organizzazione che prevedono per servizi tecnologici l'autorizzazione da parte dei Sistemi Informativi. Considerati i possibili impatti sulla sicurezza IT e sulla protezione dei dati personali è necessario informare preventivamente il CISO e il Privacy Officer / DPO per provvedere agli eventuali adempimenti di legge.
2) L'utilizzo di sistemi o servizi basati su tecnologia cloud o web non autorizzati e tracciati è considerato "incidente alla sicurezza" con tutti i risvolti sanzionatori ed eventualmente risarcitori a carico dell'utilizzatore.
3) Ai sensi di quanto previsto dalla regolamentazione ACN non è possibile per una PA acquisire servizi in modalità SaaS se non qualificati e pubblicati nel rispettivo Marketplace.

Art. 27-bis – Utilizzo di sistemi di Intelligenza Artificiale

1) Definizione
   Ai fini del presente Regolamento, per sistemi di Intelligenza Artificiale (IA) si intendono applicazioni, servizi o piattaforme software in grado di generare, analizzare, elaborare o suggerire contenuti, testi, immagini, dati o informazioni mediante processi automatizzati, inclusi assistenti virtuali e strumenti di supporto intelligente.
2) Principi generali di utilizzo
   L'utilizzo dei sistemi di Intelligenza Artificiale nell'ambito delle attività lavorative dell'Ente è ammesso esclusivamente nel rispetto:
   a) del presente Regolamento;
   b) della normativa vigente, con particolare riferimento alla protezione dei dati personali, Regolamento (UE) 2024/1689 – AI Act - Legge 23 settembre 2025, n. 132;
   c) delle policy di sicurezza informatica e delle procedure interne adottate dall'Ente.
   d) del principio di supervisione umana, garantendo che ogni contenuto, analisi, proposta, elaborazione o output generato dai sistemi di Intelligenza Artificiale sia sottoposto a verifica, validazione e valutazione critica da parte dell'operatore competente prima del relativo utilizzo nell'attività amministrativa, restando in ogni caso escluse forme di delega automatica delle decisioni, delle valutazioni discrezionali e delle responsabilità attribuite ai dipendenti e agli organi dell'Ente;
   e) del principio di responsabilizzazione (accountability), assicurando che l'Ente documenti, in misura proporzionata alla natura e ai rischi dei sistemi di Intelligenza Artificiale utilizzati, le valutazioni effettuate in merito alle finalità del trattamento, ai rischi individuati, alle misure organizzative e tecniche adottate, nonché alle verifiche svolte per garantire un utilizzo sicuro, trasparente e conforme alla normativa vigente.

3) Strumenti di riferimento e piattaforme autorizzate
   L'Ente:
   a) individua in Microsoft Copilot, correttamente licenziato, configurato, autorizzato dall'Ente e integrato nelle soluzioni Microsoft 365 adottate, lo strumento di riferimento per l'utilizzo dell'Intelligenza Artificiale in ambito lavorativo, in quanto operante all'interno del perimetro tecnologico e di sicurezza istituzionale. L'utilizzo di Microsoft Copilot è consentito esclusivamente nelle configurazioni, licenze, funzionalità e modalità operative preventivamente approvate dall'Ente e nel rispetto delle disposizioni interne vigenti in materia di sicurezza informatica, protezione dei dati e gestione dei servizi digitali;
   b) può autorizzare l'utilizzo di ulteriori piattaforme di Intelligenza Artificiale, diverse da Microsoft Copilot, purché:
   - siano formalmente acquisite o contrattualizzate dall'Ente;

- siano state sottoposte a verifica di conformità normativa, con particolare riferimento al Regolamento (UE) 2016/679 (GDPR), Regolamento (UE) 2024/1689 – AI Act - Legge 23 settembre 2025, n. 132 – Linee Guida AGID in materia;
- siano oggetto, ove previsto, di valutazione d'impatto sulla protezione dei dati (DPIA e/o FRIA);
- risultino conformi alle disposizioni interne in materia di sicurezza informatica, gestione dei dati e utilizzo dei servizi IT.

4) Utilizzo di sistemi non autorizzati
L'utilizzo di sistemi di Intelligenza Artificiale non rientranti tra quelli autorizzati ai sensi del comma 3 è consentito esclusivamente previa autorizzazione dei Sistemi Informativi, sentito il Privacy Officer / Data Protection Officer (DPO), nel rispetto delle disposizioni in materia di servizi IT esterni e di cloud computing.

5) Divieti
In assenza di specifica autorizzazione, è vietato l'inserimento, la comunicazione o il trattamento, tramite sistemi di Intelligenza Artificiale esterni, di:
a) dati personali;
b) dati personali di natura particolare;
c) informazioni riservate o confidenziali;
d) dati coperti da segreto d'ufficio;
e) informazioni relative a procedimenti amministrativi non pubblici.

6) Finalità di utilizzo
I sistemi di Intelligenza Artificiale possono essere utilizzati esclusivamente per finalità di supporto:
a) operativo;
b) redazionale;
c) informativo;
d) di miglioramento della produttività.
In ogni caso, l'utilizzo di tali sistemi non può in alcun modo:
- sostituire le valutazioni professionali degli operatori;
- incidere sull'assunzione di responsabilità individuali;
- determinare decisioni amministrative;
- generare atti aventi rilevanza giuridica senza preventiva validazione umana.

7) Responsabilità dell'utilizzatore
L'utilizzatore rimane pienamente responsabile dei contenuti prodotti, verificati, utilizzati o diffusi mediante sistemi di Intelligenza Artificiale ed è tenuto a:
a) verificarne l'accuratezza, l'affidabilità e la coerenza;
b) garantirne la conformità al quadro normativo vigente;
c) assicurare il rispetto delle disposizioni interne in materia di sicurezza e protezione dei dati.
d) I dipendenti autorizzati all'utilizzo di sistemi di Intelligenza Artificiale sono tenuti a partecipare alle attività di formazione e sensibilizzazione organizzate dall'Ente, finalizzate a garantire la conoscenza dei principi normativi applicabili, dei rischi in materia di protezione dei dati personali e sicurezza informatica, nonché delle modalità di verifica e validazione degli output generati dai sistemi di Intelligenza Artificiale prima del loro utilizzo nell'attività amministrativa.

8) Violazioni
L'uso dei sistemi di Intelligenza Artificiale in violazione delle disposizioni del presente articolo:
a) costituisce violazione del presente Regolamento;
b) è qualificabile come incidente di sicurezza;
c) comporta l'applicazione delle sanzioni previste ai sensi della normativa vigente e del Regolamento disciplinare dell'Ente.

9) Registro dei sistemi di IA
Al fine di garantire trasparenza, tracciabilità e responsabilizzazione nell'utilizzo dei sistemi di Intelligenza Artificiale, l'Ente istituisce e mantiene aggiornato un Registro degli strumenti di IA autorizzati, contenente almeno l'indicazione del fornitore, delle finalità perseguite, delle strutture

utilizzatrici, delle categorie di dati trattati, delle valutazioni di conformità e di rischio effettuate, delle misure di mitigazione adottate e dei riferimenti agli eventuali atti autorizzativi interni.

Art. 28. - Utilizzo Reti Wi-Fi pubbliche

1) Le reti Wi-Fi pubbliche con l'opzione di protezione di tipo WEP non possono essere utilizzate per ragioni di sicurezza, in considerazione del livello di riservatezza garantito. Utilizzare soltanto reti Wi-Fi che implementano protocolli di tipo WPA2 o WPA3.
2) Utilizzare la connessione Wi-Fi pubblica solo per effettuare navigazione informativa; non accedere mai alle piattaforme dell'organizzazione. È inoltre sconsigliato effettuare transazioni di tipo sensibile (ad es., acquisti o transazioni bancarie) su Wi-Fi di tipo pubblico. In caso di necessità optare per una connessione di tipo *Tethering* ovvero utilizzando il proprio smartphone come *gateway* Internet.

Art. 29. - Utilizzo Reti Bluetooth

1) Il Bluetooth deve essere attivato soltanto quando effettivamente necessario; alla fine della sessione di lavoro deve essere sempre disattivato.
2) Al fine di garantire un adeguato livello di sicurezza è necessario verificare l'ambiente circostante in modo da poterlo considerare sufficientemente sicuro; devono quindi essere evitati i luoghi pubblici (con potenziale promiscuità inferiore ai 50 metri).
3) La visibilità del dispositivo via protocollo Bluetooth deve essere attivata solo se necessario alla prima fase di configurazione e registrazione; poi può essere disabilitata.
4) Attivare sempre le opzioni di sicurezza come l'autenticazione e la cifratura delle comunicazioni attraverso l'implementazione di protocolli sicuri.

Art. 30. - Sistemi di Sicurezza

1) L'organizzazione, al fine di tutelare il patrimonio informativo e la continuità dei servizi, utilizza dei dispositivi di sicurezza con i quali controlla e monitora, in modalità aggregata, l'attività dei sistemi e indirettamente anche quella degli utilizzatori; tali controlli sono comunque effettuati in forme tali da precludere la possibilità di identificazione diretta dei soggetti. Al fine di poter valutare i livelli di servizio erogati ed effettuare attività di ricerca forense a seguito di eventuali attacchi, tutte le attività dei sistemi e degli utilizzatori sono salvate in appositi registri o file di log, ai quali può accedere esclusivamente il personale autorizzato e specificatamente nominato Amministratore di Sistema.
2) L'accesso ai file di log da parte del personale nominato Amministratore di Sistema può avvenire per attività di normale manutenzione, a seguito di malfunzionamenti o di degradamento dei livelli di servizio, in funzione di specifiche segnalazioni oppure nel caso di richiesta da parte dell'Autorità Giudiziaria.
3) I controlli sono effettuati evitando ingiustificate interferenze sui diritti e sulle libertà fondamentali degli utilizzatori, avendo cura di tutelare anche i soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata, nel pieno rispetto dei principi di pertinenza e non eccedenza.
4) La scelta dei criteri di protezione nei sistemi di sicurezza è tesa al giusto equilibrio tra performance e livello di salvaguardia, proporzionale ai rischi connessi con la tipologia di informazioni trattate. In alcuni casi, i controlli possono interferire con l'esperienza dell'utilizzatore di sistemi e servizi IT, ad esempio con blocchi nella navigazione, accessi non concessi, segnalazione di attività non permesse. L'utilizzatore di sistemi e servizi IT è invitato a segnalare gli elementi che ritiene possano essere migliorati (ad es., falsi positivi).
5) I sistemi di sicurezza sono configurati in modo da prevenire e bloccare operazioni considerate potenzialmente pericolose oppure non direttamente correlate all'attività lavorativa, quali l'*upload*

e/o il *download* di file o software aventi particolari caratteristiche, ad esempio dimensionali o di tipologia di contenuti; eventuali eccezioni dovranno essere segnalate ai Sistemi Informativi.

6) L'utilizzatore di sistemi e servizi IT non deve modificare, aggirare, disabilitare i controlli di sicurezza. Eventuali attività ritenute sospette comporteranno l'immediata disattivazione dell'*account* di accesso ai sistemi e servizi, fino al blocco del sistema (questo poiché è impossibile per un sistema automatico stabilire con certezza se il problema è, o meno, riconducibile ad una compromissione, presentandosi come rischio inaccettabile e non risolvibile con altri mezzi).
7) L'accesso alle infrastrutture di rete, alle attrezzature e strumenti informatici è permesso al solo personale autorizzato; il personale privo di specifica autorizzazione non può effettuare alcun accesso, anche se accompagnato; è sempre necessaria una preliminare autorizzazione e registrazione.
8) I sistemi o i dispositivi compromessi a seguito di attacco devono essere ripristinati dal personale dei Sistemi Informativi seguendo le procedure previste; la delega a terza parte necessita di specifica approvazione da parte di un soggetto Designato o dal Responsabile dei Sistemi Informativi.
9) I sistemi e gli applicativi necessitano di continui aggiornamenti che permettono di mantenere l'intera infrastruttura ad un adeguato livello di protezione e sicurezza, eliminando i difetti o le vulnerabilità note. Nonostante tutte le accortezze, alcuni aggiornamenti richiedono molto tempo, rallentano il sistema o possono esigere un riavvio. L'utilizzatore di sistemi e servizi IT deve seguire quanto richiesto dal sistema o dall'applicazione nel più breve tempo possibile al fine di ridurre i rischi legati allo specifico aggiornamento.
10) Dopo l'aggiornamento dei sistemi operativi o delle applicazioni software l'utilizzatore procede con una verifica delle funzionalità principali in modo da escludere eventuali impatti negativi sulle attività operative o sulla sicurezza. In caso di malfunzionamenti o di situazioni anche soltanto sospette provvede alla segnalazione al supporto tecnico.

Art. 31. - Sondaggi (telefonici e on-line)

1) Gli attacchi di tipo *Social Engineering* si basano sullo studio del comportamento individuale di una persona al fine di ottenere informazioni utili e funzionali agli scopi malevoli; altra modalità più subdola è il tentativo di stabilire un certo livello di fiducia con la vittima in modo che riveli in autonomia le informazioni riservate necessarie agli scopi dell'attaccante.
   Per questo motivo è vietato:
   a. Rispondere a e-mail, questionari on-line o ai sondaggi se non provenienti da fonti istituzionali verificate e autorizzate (connessione in https e certificato valido);
   b. Rispondere a interviste telefoniche anche se annunciate o provenienti dall'estero (eventualmente procedere con un *call-back* verificando sul web gli eventuali chiamanti), specialmente nel caso di richieste di informazioni relative all'organizzazione, alle infrastrutture o ai prodotti tecnologici utilizzati.

Art. 32. - Accesso remoto (VPN)

1) L'acceso dall'esterno alla rete dell'organizzazione può avvenire soltanto in due modi:
   a. Utilizzando le piattaforme esposte sul web (ad es., Posta elettronica, Sito web, portale dipendenti, software applicativi JENTE, CIVILIA.NEXT, e software interni esposti e nativi web autorizzati dal Responsabile dei Sistemi Informatici dell'Ente.);
   b. Virtual Private Network (VPN) esclusivamente con doppio fattore di autenticazione (2FA);
   c. Tunnel IPSec (connessione di tipo *Site-To-Site*).
2) La richiesta di attivazione di una VPN/Tunnel IPSec deve essere presentata dal diretto superiore dell'utilizzatore inviando lo specifico modulo al supporto tecnico dei Sistemi Informativi. Devono inoltre essere specificate le macchine server o i dispositivi da raggiungere. A meno di

particolarissime eccezioni autorizzate dal Responsabile dei Sistemi Informativi, non sono fornite VPN/Tunnel IPSec ad accesso ampio o completo della rete dell'organizzazione.

3) L'autorizzazione deve essere rinnovata di anno in anno sempre attraverso la procedura di abilitazione. Gli *account* VPN non rinnovati sono automaticamente disabilitati alla fine del periodo.
4) La macchina su cui installare il client VPN o le macchine afferenti ad un Tunnel IPSec deve essere:
    a. Protette da password di una certa complessità;
    b. Esenti da applicativi software non licenziati, prive di *crack* di sblocco delle applicazioni o dei componenti;
    c. Aggiornate all'ultima versione disponibile di sistema operativo (i sistemi operativi in *out of support* devono essere dotati di sistema di *virtual patching* o comunque sostituiti/aggiornati il prima possibile);
    d. Dotate di software antivirus, con basi di definizione aggiornate almeno giornalmente.
5) Il software VPN disconnette automaticamente l'utilizzatore dopo 60 minuti di inutilizzo della linea. È necessario effettuare di nuovo l'accesso per ristabilire la connessione. Non sono ammessi client di accesso se non quelli distribuiti/indicati nella fase di rilascio delle credenziali di accesso.
6) Gli utilizzatori delle connessioni VPN/Tunnel IPSec, dato che sono a tutti gli effetti estensioni della rete dell'organizzazione, devono sottostare in tutto e per tutto alle disposizioni del presente Regolamento.
7) Il team di sicurezza effettua periodici monitoraggi delle attività degli utilizzatori del servizio VPN/ Tunnel IPSec attraverso *walk-thrus*, report, audit interni o esterni. Eventuali comportamenti non conformi o anche solamente sospetti negli accessi o durante le sessioni di lavoro, comporteranno l'immediata disconnessione e disabilitazione dell'*account* di connessione.
8) In caso di compromissione del sistema a causa di virus o *malware*, l'utilizzatore non deve collegarsi alla rete dell'organizzazione via VPN/Tunnel IPSec ma provvedere alla completa reinstallazione del sistema operativo, degli applicativi e componenti, servendosi soltanto di pacchetti di installazione scaricati da fonti affidabili e correttamente licenziati.
9) È permesso il salvataggio temporaneo dei file e documenti di lavoro nella postazione di proprietà personale a patto di provvedere quanto prima alla completa eliminazione, avendo cura di svuotare anche il cestino.

Art. 33. - Controllo remoto

1) Parte dell'attività di supporto tecnico è effettuata attraverso sessioni di controllo remoto, sempre su specifica attivazione/autorizzazione da parte dei singoli utilizzatori. Questa modalità permette un enorme risparmio di tempo, risposte più brevi, facilità di comprensione e risoluzione dei problemi. Anche le sessioni di *learning by doing* sono effettuate in questa modalità, conformemente al detto confuciano "*Se ascolto dimentico, se vedo ricordo, se faccio capisco*". Gli strumenti di controllo remoto aprono delle porte verso l'esterno della rete dell'organizzazione, da considerare intrinsecamente potenziale elemento di insicurezza, da regolamentare, controllare e governare.
2) Dato che gli strumenti di controllo remoto permettono di visualizzare a distanza delle attività che gli operatori effettuano con i sistemi informatici, è fondamentale che:
    a) sia sempre l'utilizzatore a richiedere il supporto tecnico (interno o esterno) tramite controllo remoto, autorizzando specificatamente ogni sessione;
    b) al termine dell'attività di supporto o formazione tramite controllo remoto, lo stesso utilizzatore provveda alla disconnessione del sistema remoto, al fine di evitare inutili occupazioni di banda e peggio la trasmissione (remota) della propria successiva attività lavorativa.
3) I tecnici interni possono utilizzare esclusivamente gli strumenti omologati dai Sistemi Informativi dell'organizzazione e pubblicati nella specifica procedura di Controllo remoto; è sempre vietata

l'impostazione di sessioni sempre attive di controllo remoto, l'utilizzo o l'installazione di strumenti alternativi a quelli previsti.

4) Eventuali eccezioni dovranno essere specificatamente autorizzate dal Responsabile dei Sistemi Informativi, poiché sono da considerarsi potenziali vulnerabilità nella rete dell'organizzazione.
5) Al fine di ridurre la superficie di esposizione e le vulnerabilità connesse all'utilizzo di strumenti di controllo remoto saranno effettuati periodici scanning di rete in modo da verificare la presenza di applicazioni di controllo remoto non autorizzate o sempre attive. Le applicazioni di controllo remoto non conformi saranno rimosse.

Art. 34. - Pubblicazione di informazioni sui siti web istituzionali e Social media

1) Il Comune di Senigallia utilizza i propri siti web e i social media dell'organizzazione per informare, comunicare, ascoltare e per consentire una relazione più diretta e una maggiore partecipazione dei clienti.
2) Attualmente la comunicazione istituzionale del Comune di Senigallia avviene attraverso le pagine tematiche presenti su:
    a. https://www.comune.senigallia.an.it
    b. Facebook https://www.facebook.com/comune.senigallia

    In futuro non sono escluse ulteriori affiliazione ai social media (la lista delle piattaforme attive è pubblicata nell'header e/o nel footer del sito web istituzionale) o la registrazione di specifici domini web tematici.
3) I contenuti pubblicati sui siti web istituzionali e sui social possono comprendere comunicazioni sulle attività e i servizi erogati, comunicati stampa, pubblicazioni e documenti ufficiali, novità normative, informazioni su iniziative ed eventi di settore, immagini e video istituzionali e relativi a eventi a cui l'organizzazione partecipa.
4) I canali producono propri contenuti testuali, fotografie, informazioni grafiche, video e altri materiali multimediali che sono da considerarsi in licenza *Creative Commons* CC BY-ND 4.0 [Attribuzione – Non opere derivate https://creativecommons.org/licenses/by-nd/4.0] così come approvata con Deliberazione di Giunta 149 del 01/07/2025: possono essere riprodotti liberamente, ma devono sempre essere accreditati al canale originale di riferimento.
5) I commenti e i post degli utenti, presentati preferibilmente con nome e cognome non fittizi, rappresentano l'opinione dei singoli e non quella dell'organizzazione, che non può essere ritenuta responsabile della veridicità o meno di quanto postato sui canali da terzi, entità giuridiche o naturali.
6) I partecipanti alle discussioni sui social network sono responsabili dei contenuti pubblicati e delle opinioni espresse. Non sono comunque tollerati insulti, volgarità, offese, minacce. Devono essere evitati riferimenti a fatti o a dettagli privi di rilevanza pubblica, atteggiamenti violenti, offensivi o discriminatori rispetto al genere, orientamento sessuale, età, religione, convinzioni personali, origini etniche, disabilità. Eventuali messaggi contenenti dati personali (indirizzi e-mail, numeri di telefono, numeri di conto corrente, indirizzi, etc.), o dati di tipo particolare, come anche informazioni riservate o confidenziali relative all'organizzazione, saranno rimossi a tutela delle persone interessate.
7) L'attività di moderazione da parte dell'amministratore della piattaforma o del social può avvenire solo a posteriori in un momento successivo alla pubblicazione; l'attività è finalizzata, unicamente, al contenimento di eventuali comportamenti contrari alle norme d'uso, garantendo a tutti il diritto di intervenire ed esprimere la propria libera opinione. L'operatore può utilizzare il *nickname* previsto oppure utilizzare il proprio nominativo e, in tal caso, è tenuto a rivelare anche la sede di lavoro e la mansione ricoperta.

8) Non sono tollerati comportamenti da cosiddetti *hater*, con insulti, turpiloquio, minacce o atteggiamenti che ledano la dignità personale, i diritti delle minoranze e dei minori, i principi di libertà e uguaglianza o altri principi costituzionalmente riconosciuti ed in particolare:
    a. Contenuti che promuovono, favoriscono, o perpetuano la discriminazione sulla base del sesso, della razza, della lingua, delle opinioni politiche, credo religioso, età, stato civile, nazionalità, disabilità fisica o mentale, orientamento sessuale;
    b. Contenuti sessuali o *link* (collegamenti) a contenuti sessuali;
    c. Pubblicità evidente o sollecitazioni commerciali;
    d. Incoraggiamento ad attività illecite;
    e. Informazioni che possono tendere a compromettere la sicurezza o la sicurezza dei sistemi pubblici;
    f. Contenuti che violino l'interesse di una proprietà legale o di terzi;
    g. Commenti o post che presentino dati sensibili in violazione della normativa sulla protezione dei dati personali;
    h. Sono inoltre scoraggiati e comunque soggetti a moderazione commenti e contenuti dei seguenti generi:
        i. Spam, commenti non pertinenti agli argomenti trattati (*off topic*);
        ii. Osservazioni pro o contro campagne politiche o indicazioni di voto;
        iii. Linguaggio o contenuti offensivi;
        iv. Commenti e i *post* scritti per disturbare la discussione, offendere chi gestisce e modera i canali social;
        v. Interventi inutili o inseriti ripetutamente.
9) Gli utilizzatori che dovessero violare ripetutamente le condizioni sopra riportate o quelle contenute nelle specifiche *policy* degli strumenti adottati, potranno essere "*bannati*" o bloccati al fine di impedirne ulteriori interventi.
10) Le attività ritenute illegali saranno immediatamente comunicate alle autorità competenti.

Art. 35. - Formazione

1) L'utilizzatore di sistemi e servizi IT è tenuto a frequentare i corsi frontali, *blended* o in modalità e-learning considerati prerequisito di accesso ai servizi e agli applicativi, come anche di aggiornamento a seguito di introduzioni di novità rilevanti, siano essi organizzati dai Sistemi Informativi, tenuti dal personale interno o da esperti esterni.
2) L'utilizzatore di sistemi e servizi IT che compia azioni vietate dal presente Regolamento, è obbligato a frequentare una specifica sessione di formazione dedicata ai temi connessi con la non conformità riscontrata, di concerto con il Dirigente della UO di riferimento. La sessione formativa è organizzata a cura dei Sistemi Informativi o attraverso l'adesione a specifici percorsi formativi dedicati al digitale come ad esempio il Progetto Nazionale Syllabus.
3) A conclusione di ogni intervento formativo (prerequisito, aggiornamento o *retraining*) potrà essere prevista la verifica delle competenze acquisite tramite test di valutazione. Nel caso in cui l'utilizzatore di sistemi e servizi IT non superi la prova con almeno l'80% delle risposte esatte, è obbligato a ripetere la formazione e il test, senza la possibilità temporanea di accesso all'ambiente di produzione del servizio o applicativo oggetto della formazione. Ove disponibile e se previsto, è possibile utilizzare specifici ambienti di simulazione per il miglioramento delle competenze.
4) Il Responsabile dei Sistemi Informativi, al fine di migliorare il livello di sicurezza, organizza con cadenza annuale delle sessioni di formazione ed aggiornamento dedicate al personale IT sui temi della sicurezza IT e protezione dati personali, nonché su temi specifici connessi ai compiti di Amministratore di sistema.

CAPO III – Attori e ruoli

Art. 36. - Utilizzatore dei servizi e degli applicativi

1) L'Utilizzatore dei servizi e degli applicativi è un individuo espressamente autorizzato ad effettuare trattamenti di dati attraverso applicazioni software. Le autorizzazioni possono essere nominali o per funzione ovvero per appartenenza a uno specifico gruppo di lavoro.
2) Le autorizzazioni sono concesse dal Dirigente di Unità Operativa che individua ambito e profilo di autorizzazione con comunicazione al personale dei Sistemi Informativi, che di conseguenza provvede alle necessarie impostazioni a livello di sistema o di applicativo.
3) L'Utilizzatore dei servizi e degli applicativi deve attenersi scrupolosamente alle procedure operative indicate nei manuali d'uso, nelle note operative, negli aiuti in linea, illustrati durante le sessioni formative o comunicate durante il cosiddetto *learning by doing (*cd. "imparare facendo"*).*
4) Gli utilizzatori dei servizi e degli applicativi hanno l'obbligo di segnalare immediatamente al proprio Dirigente qualsiasi evento o situazione di rischio della sicurezza dei sistemi e delle reti di comunicazione, al fine di tutelare il patrimonio informativo dell'organizzazione e garantire la necessaria continuità operativa.

Art. 37. - Amministratori di Sistema (AdS)

1) Il personale sistemistico e di networking, avendo facoltà di accesso alle informazioni anche senza i vincoli e le protezioni del livello applicativo, è nominato Amministratore di Sistema dal Responsabile dei Sistemi Informativi o dal Dirigente/Responsabile Unità Operativa che provvede ad attribuire singolarmente l'ambito di autorizzazione. Sono considerati Amministratori di sistema i tecnici che lavorano a tutti i livelli della catena tecnologica, di solito al di sotto dello strato applicativo inclusi coloro che possono definire e rilasciare credenziali di autenticazione ad altri soggetti.
2) A partire dal livello "visibile", la catena tecnologica è composta da:
    a. Livello applicativo;
    b. Middleware (DBMS e web service);
    c. Sistemi operativi;
    d. Hypervisor;
    e. Server e sottosistemi SAN/NAS;
    f. Network.
3) I principali compiti di un Amministratore di Sistema sono i seguenti:
    a. Monitorare l'infrastruttura informatica di competenza attraverso l'analisi dei log, identificando e prevenendo potenziali problemi;
    b. Introdurre ed integrare nuove tecnologie negli ambienti esistenti;
    c. Installare e configurare nuovo hardware/software sia lato client, sia lato server;
    d. Applicare le patch e gli aggiornamenti necessari al software di base ed applicativo, modificare le configurazioni in base alle esigenze dell'organizzazione;
    e. Gestire e tenere aggiornati gli *account* utente ed i relativi profili di autorizzazione;
    f. Fornire risposte alle questioni tecniche sollevate dall'utenza, porre rimedio ai problemi/guasti tramite tecniche di *troubleshooting*;
    g. Pianificare e verificare la corretta esecuzione dei backup e delle repliche;
    h. Documentare le operazioni effettuate (*Logbook*), le configurazioni, le modalità di backup e di ripristino dei dati e dei sistemi, gli eventi e le soluzioni ai problemi;
    i. Ottenere le migliori prestazioni possibili con l'hardware a disposizione;
    j. Effettuare controlli tecnici a tutti i livelli della catena tecnologica per verificare funzionalità e sicurezza di singoli sistemi, dispositivi e applicazioni software, secondo le modalità previste dalle procedure interne;

k. Operare secondo le prescrizioni di sicurezza, le indicazioni del CISO e le procedure interne previste.

Art. 38. - Fornitori di prodotti e servizi

1) I fornitori di prodotti e servizi dei Sistemi Informativi sono coloro che provvedono all'approvvigionamento di beni o alla prestazione di servizi funzionali alla missione dell'organizzazione. In fase di appalto, dichiarano di accettare le regole e le procedure del presente Regolamento.
2) In caso di *outsourcing* di un servizio relativo a un sistema oppure ad un applicativo, il personale tecnico è nominato Amministratore di Sistema dal titolare dell'azienda appaltatrice, che nello specifico svolge il ruolo di Responsabile (esterno) del trattamento ai sensi dell'art. 28 del GDPR. Almeno una volta l'anno, il titolare dell'azienda appaltatrice comunica al Responsabile dei Sistemi Informativi l'elenco degli Amministratori di Sistema nominati e autorizzati a effettuare le attività legate al servizio oggetto dell'appalto.

Art. 39. - Privacy Officer / Data Protection Officer (DPO)

1) Il Privacy Officer / DPO ha le seguenti responsabilità (oltre a quanto già previsto dall'art 39 del GDPR):
    a. Sensibilizzare e formare il personale in modo da garantire un adeguato livello di consapevolezza sulle minacce alla sicurezza informatica;
    b. Supportare il Comune, titolare del trattamento, nella gestione delle procedure di data breach;
    c. Fungere da punto di contatto con l'Autorità Garante della protezione dei dati personali.

Art. 40. - Chief Information Security Officer (CISO) / Responsabile Sicurezza Informatica

1) Il Responsabile della Sicurezza Informatica o Chief Information Security Officer (CISO) ha le seguenti responsabilità:
    a. Definire la strategia di sicurezza dell'organizzazione, con il coinvolgimento della Direzione nelle scelte, nella definizione del budget e delle priorità, nella implementazione;
    b. Gestire la conformità alle norme cogenti e volontarie (se previste) definendo i requisiti necessari e verificandoli attraverso specifici audit;
    c. Proporre i documenti principali sulla sicurezza delle informazioni come politiche, regole, e corrette procedure, aggiornandoli e revisionandoli ove necessario per un utilizzo sicuro dei servizi, sistemi e dispostivi forniti dall'organizzazione;
    d. Valutare e gestire i rischi, proponendo miglioramenti e azioni correttive, assicurandosi che siano implementati in ottica di miglioramento continuo;
    e. Migliorare la consapevolezza degli utilizzatori attraverso interventi di formazione e sensibilizzazione per una cultura della sicurezza delle informazioni;
    f. Effettuare un report annuale sullo stato della sicurezza, da consegnare alla Direzione;
    g. Effettuare la redazione del piano di Business continuity, coordinandone esercizio e test;
    h. Essere in prima linea nella gestione degli incidenti e delle emergenze, coordinando il Cyber Security Team, gestendo le risposte nonché le eventuali segnalazioni alle Autorità competenti.

CAPO IV – Gestione dei servizi IT (*IT Service Management*)

Art. 41. - Catalogo dei servizi IT (*Service Design*)

1) La richiesta di un qualsiasi servizio IT erogato dai Sistemi Informatici dell'Ente, dovrà essere tracciato attraverso il sistema di *ticketing* dell'organizzazione, le cui modalità operative sono

descritte nei manuali d'uso del sistema. Tale monitoraggio consentirà una più efficiente allocazione delle risorse umane e strumentali necessarie garantire il supporto tecnico informatico dell'organizzazione.

Art. 42. - Base di conoscenza (*knowledge base*)

1) La "*Base di conoscenza*" è un contenitore adibito alla conservazione delle informazioni utili e necessarie al buon funzionamento del sistema informativo dell'organizzazione nonché per scopi culturali o didattici, con l'obiettivo di colmare il *gap* di competenze digitali degli utilizzatori.
2) Sono disponibili i seguenti materiali:
    a. Manuali utente delle piattaforme e degli strumenti in uso;
    b. Procedure IT e di gestione delle emergenze;
    c. Trucchi e suggerimenti per la risoluzione dei problemi;
    d. Articoli, report, link esterni;
    e. Link alla piattaforma e-learning per singoli "oggetti di apprendimento";
    f. FAQ.
3) L'utilizzatore è invitato a consultare la "*Base di conoscenza*"/"Sezione Formazione" disponibile nella intranet aziendale, ogni qualvolta si presentino dei problemi nell'utilizzo degli strumenti in uso e comunque prima dell'apertura di una qualsiasi richiesta, segnalazione o *ticket* al supporto tecnico.
4) I tecnici sono altresì obbligati ad aggiornare ed integrare la "*Base di conoscenza*" in modo che le informazioni presenti possano aiutare gli utilizzatori a risolvere velocemente e in autonomia le problematiche più semplici.

Art. 43. - Gestione dei cambiamenti (*Change Management*)

1) Le modifiche, sostituzioni, integrazioni dei sistemi, dispositivi, accessori, applicazioni sono gestite in modo efficiente dal personale specialistico utilizzando metodi e procedure standardizzati, in modo da ridurre al minimo i rischi per l'infrastruttura IT. Non sono ammessi cambiamenti che non seguano le procedure previste o effettuati in autonomia dagli utilizzatori.
2) Un cambiamento, ovvero un evento che si traduce in un nuovo stato di uno o più elementi di configurazione, può essere richiesto dall'utilizzatore o può risultare necessario per risolvere delle specifiche problematiche, come anche nell'ambito degli aggiornamenti e della gestione controllata della obsolescenza dell'infrastruttura IT.
3) Al fine di garantire un impatto minimo sui processi, tutti i cambiamenti sono programmati in accordo con gli utilizzatori coinvolti, contemperando la disponibilità ed economicità delle risorse nonché la continuità dei servizi.
4) A completamento delle attività di cambiamento, sono effettuati test di validazione al fine di verificare che tutti gli elementi della catena delle dipendenze funzionino perfettamente. Per i sistemi critici, i test di validazione sono effettuati seguendo apposite procedure e compilando le previste *check-list*.
5) Nell'ambito della gestione degli asset dell'infrastruttura IT, il personale impiegato nelle attività di gestione dei cambiamenti provvede all'integrazione e aggiornamento della documentazione tecnica.

Art. 44. - Erogazione del servizio di Supporto tecnico (*Service Operation*)

1) L'erogazione del servizio di supporto tecnico è basata su risorse e priorità. Questo perché le risorse non sono infinite ed è necessario trovare un equilibrio tra costi e affidabilità del servizio, con specifico riferimento ai tempi di risposta, possibilmente rientrando nei livelli di servizio concordati (SLA).
2) La gestione delle priorità è basata sul livello di criticità dei servizi, contraddistinta con la seguente codifica a colori:

ROSSO: sistemi e servizi critici, *front-office*, gestione emergenze;

GIALLO: sistemi e servizi secondari (ad es., amministrazione);

VERDE: sistemi e servizi con problematiche non bloccanti.

3) Gli SLA previsti sono i seguenti (comunque a meno di specifiche situazioni di emergenza da segnalare al personale dei Sistemi Informativi):

   ROSSO: presa in carico immediata attraverso chiamata telefonica o apertura ticket tempo di risoluzione del problema: entro 4 ore nel 96% dei casi;

   GIALLO: presa in carico entro 4 ore attraverso esclusivamente l'apertura di un ticket tempo di risoluzione del problema: entro 48 ore nel 96% dei casi;

   VERDE: presa in carico entro 8 ore attraverso esclusivamente l'apertura di un ticket tempo di risoluzione del problema: entro 7 giorni nel 96% dei casi.

4) Ad ogni richiesta di intervento è associato un ticket, consultabile dal personale tecnico e dagli utilizzatori richiedenti. Il ticket è preso in carico dal singolo tecnico, specialista nella tipologia di intervento richiesto. Il ticket può essere chiuso dal tecnico che prende in carico l'intervento nel caso non si evidenzino le problematiche segnalate dall'utilizzatore oppure nel momento successiva alla risoluzione.
5) Nel caso il problema si ripresenti, l'utilizzatore deve riaprire un secondo ticket, facendo riferimento al fatto di aver già segnalato il problema.
6) Le attività del personale dei Sistemi Informativi sono esclusivamente attivate a seguito dell'apertura di un ticket tramite il sistema di help desk. Non sono prese in carico richieste informali o dirette (verbali, telefoniche o via e-mail) non precedute dall'apertura di un ticket. A seguito dell'apertura del ticket, l'utente potrà essere contattato dal personale tecnico per le necessarie attività di approfondimento oppure ricevere riscontro direttamente tramite il sistema di ticketing.
7) L'apertura del ticket è condizione necessaria per il tracciamento delle attività svolte, per la corretta attribuzione delle priorità di intervento e per la misurazione delle performance del servizio di supporto tecnico e del personale impiegato.
8) Il personale tecnico ha facoltà di accesso ai dispositivi e alle informazioni essendo stato nominato Amministratore di Sistema. L'accesso può avvenire con proprie credenziali o tramite sessioni di controllo remoto, avendo cura di non accedere per nessun motivo ad informazioni riservate, personali o particolari.

Art. 45. - Controlli (*Service Improvement*)

1) Al fine di migliorare i livelli di servizio è necessario effettuare sia le misurazioni riportate all'articolo precedente come anche analizzare i dati acquisiti e procedere con l'implementazione delle attività correttive o integrative.
2) I controlli riguarderanno sia il personale dei sistemi informativi che gli utilizzatori, a partire dalla richiesta fino alla chiusura del ticket nonché alla valutazione del servizio fornita dopo la chiusura dell'intervento.
3) I controlli potranno inoltre riguardare anche i sistemi, dispositivi, accessori o applicazioni interessate dalla richiesta di intervento o comunque in qualche modo coinvolte.
4) I livelli di servizio erogati sono pubblicati nella specifica sezione della Intranet dell'organizzazione.

CAPO V – Prescrizioni per gli utilizzatori/lavoratori agili/telelavoratori/ lavoratori in mobilità

Art. 46. - Orari di erogazione dei servizi

1) I servizi informatici e la connettività alla rete Internet, a meno di malfunzionamenti, emergenze o attività di manutenzione, sono disponibili durante il normale orario di lavoro. È possibile che in alcuni casi siano attive delle restrizioni, imposte per motivi di sicurezza, tali da non permettere l'accesso da paesi extra UE o in orari al di fuori da quelli stabiliti contrattualmente con il personale dipendente. Eventuali eccezioni nell'erogazione o nella fruizione dovranno essere espressamente autorizzate dal Dirigente dell'UO, sentito il Responsabile dei Sistemi Informativi.
2) Le attività di manutenzione dei sistemi dovranno essere comunicate con congruo anticipo, a meno di specifiche situazioni di emergenza (attacchi o vulnerabilità cd. "*zero day*") e dovranno concludersi entro le tempistiche previste.
3) L'utilizzatore del servizio organizzerà i propri tempi di lavoro in funzione dei momenti di blocco, senza la possibilità di richiedere per nessun motivo dilazioni o ritardi. Le sessioni aperte nel momento di inizio della manutenzione saranno comunque chiuse, accettando il rischio di perdita delle informazioni inserite provvisoriamente ma ancora non validate.

Art. 47. - Modalità di lavoro agile

1) Il lavoratore agile ha l'obbligo di svolgere la propria prestazione cooperando con diligenza all'attuazione delle misure di prevenzione e protezione predisposte dal datore di lavoro, al fine di fronteggiare i rischi connessi all'esecuzione della prestazione in ambienti privati *indoor* diversi da quelli dell'organizzazione. È comunque esclusa la possibilità di prestazione lavorativa in ambienti *outdoor*. A tal fine, il datore di lavoro predispone un'informativa scritta, da presentare al lavoratore e al rappresentante dei lavoratori per la sicurezza, con cadenza almeno annuale, dove sono individuati i rischi generali e specifici connessi alla particolare modalità di esecuzione del rapporto di lavoro.
2) Il lavoratore agile ha il dovere di verificare:
    a. la sicurezza antincendio dei locali utilizzati per la prestazione lavorativa, in termini di conoscenza dei principi generali del Triangolo del fuoco (combustibile, comburente e fonte d'innesco), la presenza o meno, così come la conoscenza e l'utilizzo dei mezzi di estinzione, il comportamento da tenere in caso di incendio o di presenza di atmosfere esplosive;
    b. i requisiti igienici minimi dei locali come il microclima, la temperatura e l'umidità dei locali, gli elementi di qualità dell'aria con riferimento al ricambio d'aria e alla presenza di eventuali sorgenti di emissioni, impianti termici e di condizionamento, etc.;
    c. l'efficienza e l'integrità dei dispositivi informatici prima dell'uso in modo da evitare i pericoli connessi con eventuali fili scoperti, adattatori o ciabatte non a norma, fili non adatti a sovraccarichi causati da stufette elettriche o termoconvettori, etc.;
    d. l'utilizzo corretto dei dispositivi secondo le istruzioni d'uso del produttore e la regolamentazione interna, specie per gli strumenti informatici;
    e. la conformità ai requisiti minimi di sicurezza degli impianti di alimentazione elettrica dei locali utilizzati (corretta messa a terra, presenza di un interruttore magnetotermico differenziale o salvavita);
    f. il buono stato dell'impianto elettrico e dei cavi elettrici di collegamento, il posizionamento e l'utilizzo delle prese;
    g. la presenza delle condizioni e delle caratteristiche minime relative alla ergonomia della postazione dotata di personal computer e delle modalità di utilizzo, sempre in ergonomia, dei sistemi portatili o dei tablet;

h. la conoscenza delle norme di comportamento da tenere in caso di funzionamenti anomali, guasti ai sistemi o ai dispositivi propri o forniti dall'organizzazione.

3) Il lavoratore agile, pur se situato presso la sua abitazione, deve comunque mantenere lo stesso livello di decoro di un normale lavoratore, specie nelle *video call*. Deve prevedere degli spazi che garantiscano un adeguato livello di silenzio e riservatezza. I sistemi personali in uso dovrebbero essere utilizzati esclusivamente dal soggetto utilizzatore, specie se nel sistema sono conservati dati di titolarità dell'organizzazione in forma non criptata.
4) È vivamente consigliato mantenere gli stessi ritmi lavorativi e le stesse abitudini acquisiti nel periodo di normale attività presso la sede dell'organizzazione in quanto funzionale alla qualità della prestazione lavorativa. Il tempo risparmiato nei trasferimenti da casa al posto di lavoro potrebbe essere investito dal lavoratore agile in attività motorie fondamentali sia per la salute sia per la qualità della vita.
5) In relazione all'accesso dall'esterno alla rete dell'organizzazione sono previsti i seguenti requisiti:
    a. Utilizzo delle piattaforme esposte sul web (ad es., Posta elettronica, Sito web, portale dipendente, etc.);
    b. Virtual Private Network (VPN) esclusivamente con doppio fattore di autenticazione (2FA);
    c. Terminale remoto (anche in combinazione con una VPN).
6) I servizi pubblicati sul web sono consultabili anche da dispositivi mobile come tablet o smartphone mentre la VPN è installabile soltanto su personal computer. La prestazione lavorativa con gli applicativi forniti dall'organizzazione è ammessa esclusivamente attraverso l'utilizzo del personal computer.
7) La richiesta di attivazione di una VPN deve essere presentata dal diretto superiore dell'utilizzatore inviando il previsto modulo al supporto tecnico dei Sistemi Informativi. Devono inoltre essere specificate le macchine server o i dispositivi da raggiungere e, a meno di particolarissime eccezioni autorizzate dal Responsabile dei Sistemi Informativi, non sono fornite VPN ad accesso ampio o completo della rete dell'organizzazione.
8) L'autorizzazione alla VPN deve essere rinnovata di anno in anno, sempre attraverso la procedura di abilitazione. Gli *account* VPN non rinnovati sono automaticamente disabilitati alla fine del periodo.
9) I requisiti minimi previsti per il collegamento via VPN sono riportati all'art. Accesso remoto (VPN).
10) Il salvataggio temporaneo dei file e documenti di lavoro nella postazione di proprietà personale è permesso a condizione di provvedere, il prima possibile e comunque periodicamente, alla loro completa eliminazione. Il lavoratore agile predilige i sistemi di *file hosting* dell'organizzazione ufficialmente distribuiti o modalità di lavoro in desktop remoto.

Art. 48. - Modalità di Telelavoro (o assimilabili)

1) Il telelavoro prevede l'utilizzo di sistemi e dispositivi forniti dal datore di lavoro, secondo i medesi orari previsti nelle modalità ordinarie di lavoro.
2) Le disposizioni e prescrizioni previste per i lavoratori in modalità "Telelavoro" sono le medesime riportate all'Art. 47 - "Modalità di lavoro agile", con l'unica differenza riguardante le *policy* tendenzialmente più stringenti previste per i sistemi informatici dell'organizzazione.

Art. 49. - Formazione per i lavoratori agili/telelavoratori o in modalità miste

1) Come previsto da specifico programma dell'Unione europea volto a sostenere l'istruzione e la formazione permanente, anche il lavoratore in forme alternative di lavoro ha il diritto di rimanere informato ed essere formato.[8]

[8] Quanto premesso in conformità all'art. 20 - Trattamento, diritto all'apprendimento continuo e certificazione delle competenze del lavoratore della legge 22 maggio 2017, n. 81 (Misure per la tutela del lavoro autonomo non imprenditoriale e misure volte a favorire l'articolazione flessibile nei tempi e nei luoghi del lavoro subordinato, pubblicata in GU, serie generale, n. 135 del 13 giugno 2017), che recita: «al lavoratore impiegato in forme di lavoro

2) Al fine di garantire le stesse condizioni di accesso alla formazione e di sviluppo di carriera previste per i lavoratori standard, è necessario che il lavoratore agile sia costantemente aggiornato sull'evolversi della situazione lavorativa anche con specifiche e periodiche *conference call*.
   I lavoratori convenzionali e il diretto superiore devono condividere tutti i materiali prodotti o acquisiti in specifici contenitori on-line, in modo da facilitare anche coloro che non sono presenti tutti i giorni in ufficio e permettere loro l'acquisizione del bagaglio di conoscenze necessario all'esecuzione dei compiti assegnati.
3) Per quanto riguardante la formazione, i materiali possono essere consultati attraverso le seguenti modalità:
   a. Intranet (https://cas.comune.senigallia.an.it/ Sezione "Formazione"

   Tutti i contenitori sono accessibili sia dalla rete locale che dalla rete Internet, via web o via VPN agli indirizzi specificati.
4) È necessario procedere con una certificazione periodica e formale delle competenze. La formazione effettuata attraverso strumenti di e-learning ha la stessa valenza e verificabilità delle competenze acquisite mediante la formazione frontale. Il lavoratore in forme alternative di lavoro partecipa alle sessioni formative on-line secondo gli schemi previsti e certifica le competenze acquisite attraverso specifici test di valutazione (sempre on-line) oppure attraverso colloqui frontali o via conference call.
5) La formazione in modalità e-learning o *blended* (sessioni miste on-line e frontali) può essere differenziata nella metodologia ma non nei test finali. Il lavoratore agile dopo aver partecipato a corsi in modalità e-learning sostiene i medesimi test di valutazione di un lavoratore frontale.

Art. 50. - Gestione di una conference call (*Etiquette Rules*)

1) In una riunione tramite strumenti informatici valgono le stesse regole di educazione di una riunione convenzionale frontale. Vi sono però dei vincoli e dei possibili problemi legati alle tecnologie che richiedono una particolare attenzione al fine di evitare perdite di tempo e insoddisfazione dei partecipanti.
2) È importante concordare con congruo anticipo lo strumento e il momento preciso in cui tenere la call. L'organizzatore deve inviare un invito, verificando prima le agende condivise, in modo che sia possibile attivare semplicemente con un click lo strumento prescelto per la conferenza, senza sprechi di tempo e chiamate parallele del tipo "*cosa utilizziamo per la call?*".
3) La regola generale prescrive che chi ha bisogno *cerca*, *invita* e *chiama*; viceversa, chi fornisce il supporto deve essere chiamato da colui che ha bisogno.
4) Considerati gli strumenti, le modalità e gli immancabili disturbi e disconnessioni, la call dovrebbe essere di una durata pari a 10, 20 o al massimo di 30 minuti nei quali concentrare l'essenza dei contenuti della riunione. I materiali dovrebbero essere condivisi con congruo anticipo in modo che i partecipanti possano comunque apportare il loro contributo senza discussioni o perdite di tempo; le *slide* per le presentazioni NON devono essere condivise preliminarmente ma mostrate esclusivamente nella sessione.
5) Nel caso in cui un partecipante sappia in anticipo di un probabile ritardo, è tenuto a comunicarlo all'organizzatore in modo che, se possibile, la call sia fissata in un secondo momento o posticipata.
6) Data l'impossibilità di "*multitasking*" nelle call, quando un partecipante non risponde alle chiamate o agli inviti, non è corretto insistere o lasciare messaggi (almeno la prima volta). Se dopo diversi tentativi il soggetto non risponde, è opportuno lasciare un messaggio o inviare una e-mail. A meno di particolari urgenze, l'organizzatore non dovrebbe richiamare.

agile […] può essere riconosciuto […] il diritto all'apprendimento permanente, in modalità formali, non formali o informali, e alla periodica certificazione delle relative competenze».

7) L'organizzatore dovrebbe invitare alla call il minor numero di persone possibile poiché più persone partecipano, più difficilmente verrà prestata la dovuta attenzione (a meno delle sessioni formative).
8) Tutti i partecipanti alla call devono prestare attenzione al luogo da dove è effettuata la chiamata, ovvero in ambiente tranquillo, senza rumori di fondo e sempre supportati da una buona connettività (di solito il Wi-Fi, ad esempio in giardino, non permette un livello di qualità audio e video accettabile); sono esclusi luoghi pubblici, in presenza di altre persone, anche se familiari, specie nel caso di trattazione di temi dell'organizzazione, delicati o comunque sottoposti a segreto di ufficio.
9) Ad esclusione dell'organizzatore, tutti i partecipanti si accertano di tenere chiusa (in modalità *mute*) la comunicazione audio in modo da evitare rumori di fondo o effetti Larsen (feedback acustico o ritorno); il passaggio da muto a microfono attivo è effettuato dal partecipante solo in caso di richiesta di intervento o per richiedere la parola.
10) In caso di utilizzo di sistemi di comunicazione nuovi, non conosciuti, è opportuno accertarsi preliminarmente dei prerequisiti tecnici (installazione di applicazioni software, componenti, plug-in, livelli audio) ed effettuare almeno un test preliminare prima dell'inizio della call.
11) Nelle prime sessioni di *conference* è preferibile utilizzare la versione video con la ripresa delle persone sfruttando la possibilità di conoscersi, specie se non se ne è avuta occasione in precedenza; per le successive sessioni può essere considerata accettabile anche la *audio conference* (senza video) con attiva la condivisione dei materiali.
12) A meno di particolari situazioni, la call deve iniziare e concludersi nei tempi stabiliti; non è corretto attendere indefinitamente i ritardatari soprattutto per non incoraggiare la loro condotta, pertanto, chi arriva in ritardo potrà essere contattato direttamente dall'organizzatore in modo da poter ricevere le informazioni perdute senza effetti negativi sugli altri partecipanti.
13) L'organizzatore della call deve mostrarsi immediatamente, presentare i partecipanti, esporre i contenuti e dare le dovute indicazioni di servizio, tra le quali il tempo previsto per la *call* ed i relativi interventi; i partecipanti devono essere a conoscenza sin da subito di ciò che l'organizzatore si aspetta da loro.
14) La modalità di comunicazione frontale e in *call* si differenzia altresì per la necessità di adottare un linguaggio più semplice, frasi concise e pause regolari tra i differenti contenuti. Questo consentirà ai partecipanti di passare oltre o, in alternativa, di porre domande.
15) L'organizzatore della call deve prestare attenzione alla stessa partecipazione, intervenendo e togliendo la parola a chi prova a monopolizzare la sessione e chiamando gli altri ad intervenire.
16) Pur avendo a disposizione altri strumenti, come il proprio smartphone, non è corretto continuare a rispondere alle e-mail o ai messaggi mentre gli altri partecipano attivamente alla sessione; eventuali altre attività lavorative devono essere posticipate dopo la call.
17) Prima della fine della sessione è necessario avvertire i partecipanti della imminente conclusione e della possibilità, da quel momento in poi, di rivolgere opportune domande.
18) L'organizzatore della call, o un soggetto nominato segretario, deve annotare ed in seguito condividere il report della sessione:
    a. Motivo della call / obiettivi;
    b. Nominativo e ruolo partecipanti;
    c. Argomenti discussi e relativi interventi;
    d. Risultanze.

CAPO VI – Gestione delle emergenze

Art. 51. - Evento di sicurezza e Risposta

5) Un Evento di sicurezza è definito come un cambio di stato avente rilevanza ai fini della gestione di un asset o di un servizio IT. Il cambio di stato potrebbe configurare l'insorgere di un

malfunzionamento, di un incidente da gestire ai sensi del successivo articolo oppure risultare come normale attività da gestire (es. completamento di un backup).

6) L'Evento di sicurezza deve essere analizzato dal personale di supporto di primo livello e, nel caso si tratti di una eccezione, deve essere assegnato al supporto di secondo livello per la prevenzione/gestione del problema o dell'incidente.
7) Il personale di supporto di primo livello gestisce gli eventi di sicurezza senza registrare ticket, a meno che vi sia una gestione automatica delle registrazioni oppure nel caso si tratti di evento potenzialmente rilevante per la continuità operativa o impattante sui livelli di servizio previsti.

Art. 52. - Incidente di sicurezza e Risposta

1) Un incidente è definito come un qualsiasi evento eccezionale non facente parte delle operatività standard di un servizio; può causare una riduzione della qualità del servizio o provocarne l'interruzione.
2) In tutti i casi di incidente di sicurezza deve essere informato il Responsabile dei Sistemi Informativi, il CISO e il Privacy Officer / DPO che, nei casi più gravi, procederanno ad informare la Direzione Generale.
3) Ai sensi di quanto stabilito all' Art. 25 - "Obblighi in materia di notifica di incidente" del D.lgs. 138/2024 i soggetti essenziali e i soggetti importanti notificano, senza ingiustificato ritardo ed entro 24 ore, al CSIRT Italia ogni incidente che ha un impatto significativo sulla fornitura dei loro servizi, secondo la specifica procedura di gestione degli incidenti.
4) Il personale di supporto di primo livello, una volta identificato l'incidente, lo registra nel sistema di *ticketing* e allerta immediatamente il personale di supporto di secondo livello; nei casi più gravi avverte la squadra di salvataggio (*rescue team*) composta anche da personale esterno specializzato nelle tecnologie coinvolte dal problema, al fine di risolvere il più velocemente possibile la situazione riportando i livelli di servizio alla condizione precedente.
5) Il *rescue team* procede alla classificazione dell'incidente effettuando una approfondita analisi e diagnosi dell'incidente, procedendo secondo delle soluzioni documentate e preimpostate o tramite attività di *workaround* (soluzione momentanea).
6) Una volta trovate le cause, risolto l'incidente riportando alla normalità il livello di servizio erogato, il rescue team procede con la chiusura dell'evento, documentando le modalità di risoluzione. È avvertito anche il Responsabile dei Sistemi Informativi che procede con le comunicazioni ai soggetti coinvolti, inclusa la Direzione Generale, il CISO e il Privacy Officer / DPO per i casi più gravi o impattanti dal punto di vista dei diritti degli interessati.

Art. 53. - Data breach e Risposta vedi rif. procedura fornita dal DPO

1) Una violazione di sicurezza sui dati personali o data breach è un evento che comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati avvenuto in modo accidentale oppure in modo illecito.
2) Ai sensi di quanto stabilito dall'art. 33 del GDPR, in caso di Data Breach è necessario seguire la prevista procedura che prevede tra l'altro, nei casi più gravi, la comunicazione all'Autorità Garante entro 72 ore dal momento in cui se ne è avuta conoscenza.
3) In tutti i casi di violazione degli elementi di riservatezza, integrità e disponibilità delle informazioni è necessario avvertire il CISO e il Privacy Officer / DPO che provvederà ad eseguire la specifica procedura e documentare l'avvenuta violazione nel registro dei Data Breach così come disciplinato dall'Allegato 17 "Processo di analisi dei data breach" al Manuale di Gestione dei flussi documentali approvato con DG 284 del 02/12/2025.

Art. 54. - Sanzioni

4) Le operazioni effettuate in palese non conformità al presente Regolamento, esporranno alle sanzioni amministrative, civili e penali previste dalla normativa vigente.
5) Il mancato rispetto o la violazione di quanto previsto dal presente Regolamento, tenuto conto del principio di proporzionalità, è perseguibile con i seguenti provvedimenti:
    a. Comunicazione dell'illecito al Datore di Lavoro/Ufficio Provvedimenti Disciplinari che provvederà all'applicazione di quanto previsto al Regolamento Disciplinare;
    b. Comunicazione alle Autorità competenti nel caso di evidenza di reati;
    c. Revoca o disabilitazione temporanea delle credenziali di autenticazione o di specifiche autorizzazioni.

Art. 55. - Prescrizioni

1) L'attività di gestione e utilizzo degli strumenti informatici e dell'infrastruttura di rete segue le norme del presente Regolamento.
2) Il presente Regolamento è distribuito a tutto il personale e a tutti gli esterni coinvolti nelle attività di utilizzo, gestione e manutenzione dei sistemi e dei dispositivi.
3) Gli utilizzatori sono informati sul presente Regolamento, pubblicato in Intranet; saranno inoltre fissate annualmente delle sessioni formative e di aggiornamento per i nuovi assunti in modalità frontale o e-learning.
4) Il personale neoassunto è tenuto allo studio del presente Regolamento prima del rilascio delle credenziali di accesso al sistema informatico dell'organizzazione.
5) Gli utilizzatori esterni devono essere debitamente informati sul presente Regolamento prima di poter accedere ai sistemi o alla rete di comunicazione, secondo le procedure previste.
6) Annualmente ed in base all'innovazione tecnologica o a sopravvenute esigenze sia organizzative che di sicurezza, si provvederà alla revisione del presente Regolamento e alle procedure allegate.

Art. 56. - Aggiornamento e revisioni

1) Gli utilizzatori possono proporre, ove ritenuto necessario, eventuali integrazioni al presente Regolamento.
2) Le proposte saranno quindi esaminate dai responsabili della fase di revisione con particolare riferimento alle figure di Responsabile dei Sistemi informativi, Privacy Officer / DPO e Responsabile della sicurezza delle informazioni (CISO).
3) Fatte salve eventuali integrazioni normative o provvedimenti delle Autorità, il presente Regolamento è soggetto a revisione almeno una volta ogni 3 anni.

Art. 57. - Allegati

1) Le Procedure dei Sistemi Informativi fanno parte integrante del presente Regolamento.
2) Le procedure sono sviluppate, raccolte e diffuse a cura dei Sistemi Informativi. Nella specifica sezione "Formazione" presente nella piattaforma Intranet dell'organizzazione sono contenute solo le ultime versioni e revisioni aggiornate.
3) Al fine di evitare disallineamenti nella distribuzione delle procedure è sconsigliata la stampa: è necessario fare riferimento sempre all'ultima versione digitale pubblicata nella piattaforma Intranet.

Art. 58. - Modulistica

1) La modulistica di riferimento aggiornata all'ultima versione e revisione è reperibile nella Intranet dell'organizzazione.

Glossario

VPN	Rete privata virtuale; modalità di collegamento sicuro alla rete dell'organizzazione
DMZ (zone demilitarizzate)	Sottorete isolata a livello fisico o logico nella quale sono pubblicati dei servizi informatici accessibili da LAN che da WAN
Hosting	Allocazione di un servizio o applicativo su un server pubblicato in Internet
Housing	Locazione di uno spazio fisico, generalmente all'interno di appositi armadi detti rack
Facility	Infrastrutture necessarie al funzionamento di un datacenter
Middleware	Software intermediari che permettono la comunicazione tra protocolli e sistemi operativi differenti
Wi-Fi	Rete wireless
instant messaging	Sistemi di comunicazione in tempo reale in rete
log	Sistema o modalità di registrazione degli eventi
Logbook	Contenitore dei log
keylogger	Malware in grado di registrare tutti i caratteri registrati da tastiera
firewall	Sistema di protezione dai pericoli della rete Internet
antispam	Sistema di filtraggio della posta indesiderata
phishing	Tipologia di attacco in cui si induce la vittima a fornire informazioni
forward	Re-invio automatico o manuale di un messaggio
CAD	Codice dell'Amministrazione Digitale
Smart card	Dispositivo hardware con potenzialità di elaborazione e memorizzazione dati in grado di garantire elevati standard di sicurezza.
SDI	Sistema di Interscambio per la Fatturazione elettronica PA
device wipe-out	Modalità di cancellazione totale o parziale dei contenuti per motivi di sicurezza di un dispositivo in caso di perdita dello stesso
Content Filtering	Filtraggio della navigazione Internet in modo da evitare siti web non allineati con gli obiettivi dell'organizzazione
Hacking	Metodi, tecniche e operazioni volte a conoscere, accedere e modificare un sistema informatico
plug-in	Programma non autonomo che interagisce con un altro programma per ampliarne o estenderne le funzionalità originarie
packet shaping	Modalità di adattamento della comunicazione in base a politiche di miglioramento del servizio
criptazione	"offuscare" un messaggio o un documento in modo da non essere comprensibile/intelligibile alle persone non autorizzate
retention	Tempistiche di conservazione dei backup
IaaS, PaaS e SaaS	Rispettivamente infrastrutture, piattaforme e software erogabili *on demand* sul cloud
Social Engineering	Studio del comportamento individuale di una persona al fine di carpire informazioni utili.
Retraining	Ripetizione della formazione prevista per uno specifico argomento
troubleshooting	Processo di ricerca logica e sistematica delle cause di un problema su un prodotto o processo affinché possa essere risolto

Appendice 1 - Password presenti nei dizionari pubblici

In ordine di frequenza rilevata:

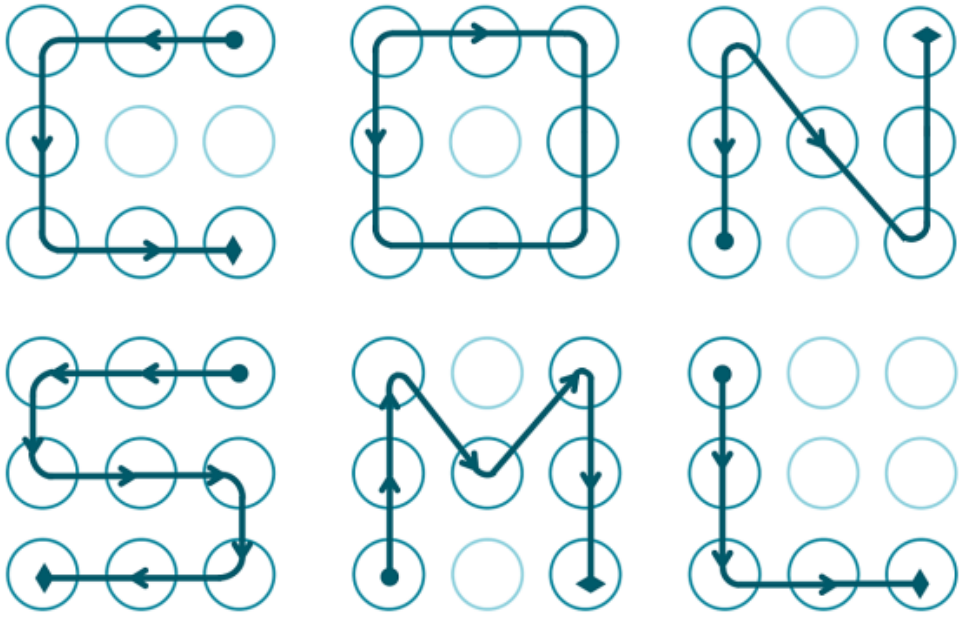
Password	123456	123456789	Qwerty	password
1111111	12345678	abc123	1234567	1234567890
9876543210	password1	12345	letmein	football
iloveyou	admin	welcome	monkey	login
starwars	123123	dragon	passw0rd	master
hello	freedom	whatever	qazwsx	trustno1

In italiano:

123456	123456789	juventus	password	12345678
ciaociao	francesca	alessandro	giuseppe	martina
francesco	valentina	qwertyuiop	antonio	stellina
federico	federica	giovanni	lorenzo	asdasd

Le password riportate in questo elenco NON DEVONO essere utilizzate.

Appendice 2 – Combinazioni "FACILI" di sblocco smartphone e tablet



Le combinazioni di sblocco riportate in questo elenco NON DEVONO essere utilizzate.

PIN più utilizzati (4 cifre)

1234	1111	0000	1212
7777	1004	2000	4444
2222	6969	9999	3333
5555	6666	1122	1313
8888	4321	2001	1010

I PIN riportati in questo elenco NON DEVONO essere utilizzati.

Appendice 3 – Categorie di *Content Filtering*

Le seguenti tipologie di siti web non sono navigabili con gli strumenti messi a disposizione dell'organizzazione:

- Adult / Mature Content
- Bandwidth Consuming
- General Interest – Business
- Potentially Liable
- Security Risk

Tali tipologie di siti web sono da considerarsi non correlate alla prestazione lavorativa.

Appendice 4 – Legislazione rilevante in ambito IT

Legge 23 dicembre 1993 n. 547 aggiornamento del Codice penale rispetto ai reati informatici

Legge 18 marzo 2008, n.48 "Ratifica ed esecuzione della Convenzione del Consiglio d' Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento interno"

Codice Amministrazione Digitale (D.lgs. 7 marzo 2005, n. 82)

Direttiva NIS (Direttiva 2016/1148) recepita attraverso il D.lgs. 18 maggio 2018, n. 65, in vigore dal 24 giugno 2018 (strategia europea per la sicurezza informatica recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione; riservato alle solo infrastrutture critiche)

Decreto del Presidente del Consiglio dei ministri 8 agosto 2019 (Decreto di costituzione del CSIRT presso la Presidenza del Consiglio dei ministri – Dipartimento Informazioni per la Sicurezza)

Regolamento (UE) 2016/679 o GDPR sulla protezione dei dati personali e D.lgs. 196/2003 novellato dal D.lgs. 101/2018

Provvedimento Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008) (modificato in base al provvedimento del 25 giugno 2009)

Direttiva 2016/680 recepita con D.lgs. 18 maggio 2018, n. 51 (sicurezza informatica dei dati trattati dalle autorità)

eIDAS (*electronic IDentification Authentication and Signature*) o Regolamento (UE) 2014/910 (sicurezza informatica applicata alla firma e alle transazioni elettroniche)

DPCM 17 febbraio 2017 o Decreto Gentiloni (delinea i nuovi assetti organizzativi dell'architettura nazionale di cyber security. Viene anche varata una nuova strategia nazionale di cyber security con l'adozione del nuovo Piano Nazionale)

Misure minime di sicurezza ICT per le pubbliche amministrazioni (Circolare 18 aprile 2017, n. 2/2017)

Circolari AgID (n. 2 e 3 del 2018)

Piano Triennale per l'informatica della PA (AgID)

Accessibilità art. 4 della Direttiva europea 2016/2102 recepita con la Legge n. 4 del 9 gennaio 2004 e successive integrazioni e modificazioni

Legge d'Autore (Legge 22 aprile 1941, n. 633, Protezione del diritto d'autore e di altri diritti connessi al suo esercizio) per la tutela del software applicativo.

D.lgs. n. 518/1992 sulla tutela giuridica del software e Legge n. 248/2000 nuove norme di tutela del diritto d'autore

D.lgs. 4 settembre 2024, n. 138 sul Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del Regolamento (UE) 2014/910 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148.

Regolamento (UE) 2024/1689 – AI Act

Legge 23 settembre 2025, n. 132

Appendice 5 – Mappa requisiti ISO/IEC 27001:2022 e articoli Regolamento IT

REQUISITI ISO/IEC 27001:2022	ARTICOLI REGOLAMENTO IT
Punto 5 - Controlli organizzativi	
Politiche per la sicurezza delle informazioni (5.1)	CAPO I - Disposizioni generali
Ruoli e responsabilità per la sicurezza delle informazioni (5.2) Separazione dei compiti (5.3)	CAPO III - Attori e ruoli
Contatti con le Autorità (5.5)	Art. 39. - Privacy Officer / Data Protection Officer (DPO)
Contatti con gruppi specialistici (5.6)	Art. 40. - Chief Information Security Officer (CISO) / Responsabile Sicurezza Informatica
Inventario delle informazioni e degli altri asset relativi (5.9)	Art. 6. - Condotta e utilizzo etico dei servizi e dei sistemi IT
Uso accettabile delle informazioni e degli altri asset relativi (5.10)	Regolamento IT Procedure IT
Restituzione degli asset (5.11)	Art. 18. - Dispositivi Mobili (smartphone, tablet e pen drive/portable disk)
Trasferimento delle informazioni (5.14)	Art. 12. - Posta elettronica convenzionale Art. 13. - Posta Elettronica Certificata (PEC) Art. 15. - Instant messaging Art. 18. - Dispositivi Mobili (smartphone, tablet e pen drive/portable disk) Art. 21. - Utilizzo del personal computer (desktop) o del portatile (laptop)
Controllo degli accessi (5.15)	CAPO II - Strumenti Art. 9. - Identificazione, autenticazione e autorizzazione Art. 10. - Registrazione delle attività (*Accounting*) Art. 11. - Corretto uso delle Credenziali di autenticazione
Gestione delle identità (5.16)	Art. 9. - Identificazione, autenticazione e autorizzazione Art. 10. - Registrazione delle attività (*Accounting*) Art. 11. - Corretto uso delle Credenziali di autenticazione
Informazioni di autenticazione (5.17)	Art. 11. - Corretto uso delle Credenziali di autenticazione
Diritti d'accesso (5.18)	Art. 9. - Identificazione, autenticazione e autorizzazione
Sicurezza delle informazioni nelle relazioni con i fornitori (5.19)	Art. 38. - Fornitori di prodotti e servizi
Gestione della sicurezza delle informazioni nella filiera di fornitura per l'ICT (5.21)	Art. 2. - Ambito di applicazione - Perimetro Art. 38. - Fornitori di prodotti e servizi
Sicurezza delle informazioni per l'utilizzo di servizi cloud (5.23)	Art. 27. - Cloud computing e servizi IT esterni
Responsabilità e procedure (5.24)	CAPO III - Attori e ruoli
Risposta agli incidenti relativi alla sicurezza delle informazioni (5.26)	CAPO VI - Gestione delle emergenze
Raccolta di prove (5.28)	Art. 10. - Registrazione delle attività (*Accounting*)
Sicurezza delle informazioni durante le interruzioni (5.29)	CAPO VI - Gestione delle emergenze
Identificazione dei requisiti legali, statutari, regolamentari e contrattuali (5.31)	Appendice 4 - Legislazione rilevante in ambito IT
Diritti di proprietà intellettuale (5.32)	Art. 20. - Navigazione Internet Art. 25. - Utilizzo delle cartelle di rete, collegate e condivise
Privacy e protezione dati personali (5.34)	Art. 5. - Principi

REQUISITI ISO/IEC 27001:2022	ARTICOLI REGOLAMENTO IT
Procedure operative documentate (5.37)	Regolamento IT Procedure IT
Punto 6 - Controlli sul personale	
Screening (6.1)	Art. 9. - Identificazione, autenticazione e autorizzazione Art. 10. - Registrazione delle attività (*Accounting*)
Termini e condizioni d'impiego (6.2)	CAPO III - Attori e ruoli
Consapevolezza, istruzione, formazione e addestramento sulla sicurezza delle informazioni (6.3)	Regolamento IT
Processo disciplinare (6.4)	Art. 54. - Sanzioni Art. 55. - Prescrizioni
Responsabilità dopo la cessazione o il cambio d'impiego (6.5)	Art. 11. - Corretto uso delle Credenziali di autenticazione
Lavoro a distanza (6.7)	CAPO V - Prescrizioni per gli utilizzatori/lavoratori agili/telelavoratori
Segnalazione degli eventi relativi alla sicurezza delle informazioni (6.8)	Art. 36. - Utilizzatore dei servizi e degli applicativi CAPO VI - Gestione delle emergenze
Punto 7 - Controlli fisici	
Perimetro di sicurezza fisica (7.1)	Art. 2. - Ambito di applicazione - Perimetro
Lavoro in aree sicure (7.6)	Art. 30. - Sistemi di Sicurezza
Schermo e scrivania puliti (7.7)	Art. 21. - Utilizzo del personal computer (desktop) o del portatile (laptop)
Disposizione delle apparecchiature e loro protezione (7.8)	Art. 21. - Utilizzo del personal computer (desktop) o del portatile (laptop)
Sicurezza degli asset all'esterno delle sedi	Art. 18. - Dispositivi Mobili (smartphone, tablet e pen drive/portable disk)
Supporti di memorizzazione (7.10)	Art. 18. - Dispositivi Mobili (smartphone, tablet e pen drive/portable disk)
Punto 8 - Controlli tecnologici	
Endpoint degli utenti (8.1)	CAPO II - Strumenti
Diritti di accesso privilegiato (8.2)	Art. 37. - Amministratori di Sistema (AdS)
Limitazione degli accessi alle Informazioni (8.3)	Art. 5. - Principi Art. 25. - Utilizzo delle cartelle di rete, collegate e condivise
Autenticazione sicura (8.5)	Art. 9. - Identificazione, autenticazione e autorizzazione Art. 10. - Registrazione delle attività (*Accounting*) Art. 11. - Corretto uso delle Credenziali di autenticazione
Raccolta di log (8.15)	Art. 10. - Registrazione delle attività (*Accounting*)
Installazione del software sui sistemi in esercizio (8.19)	Art. 18. - Dispositivi Mobili (smartphone, tablet e pen drive/portable disk) Art. 21. - Utilizzo del personal computer (desktop) o del portatile (laptop) Art. 43. - Gestione dei cambiamenti (*Change Management*)
Sicurezza dei servizi di rete (8.21)	Art. 30. - Sistemi di Sicurezza
Web filtering (8.23)	Art. 20. - Navigazione Internet Appendice 3 - Categorie di Content Filtering
Uso della crittografia (8.24)	CAPO II - Strumenti Art. 12. - Posta elettronica convenzionale
Requisiti di sicurezza delle applicazioni (8.26)	Art. 16. - Sistemi informatici Art. 17. - Applicazioni software

REQUISITI ISO/IEC 27001:2022	ARTICOLI REGOLAMENTO IT
Gestione dei cambiamenti (8.32)	Art. 43. - Gestione dei cambiamenti (*Change Management*)

Appendice 6 – Mappa requisiti Allegato 2 Det. ACN 2025/164179 e articoli Regolamento IT

REQUISITI ALLEGATO 2 DET. ACN 2025_164179	ARTICOLI REGOLAMENTO IT
a) Gestione del rischio.	GV.OC-4 punto 1: Art. 16. - Sistemi informatici
b) Ruoli e responsabilità.	GV.RR-02 punti 1, 2: CAPO III - Attori e ruoli
c) Affidabilità delle risorse umane.	GV.RR-04 punti 1, 2: CAPO III - Attori e ruoli
d) Conformità e audit di sicurezza.	GV.PO-01: CAPO I - Disposizioni generali
e) Gestione dei rischi per la sicurezza informatica della catena di approvvigionamento.	GV.SC-01 punti 1, 2: Art. 38. - Fornitori di prodotti e servizi GV.SC-02 punto 1: CAPO III - Attori e ruoli
f) Gestione degli asset.	ID.AM-01 punto 1: Art. 16. - Sistemi informatici
g) Gestione delle vulnerabilità.	ID.RA-01 punti 1, 2: Art. 16. - Sistemi informatici
h) Continuità operativa, ripristino in caso di disastro e gestione delle crisi.	ID.IM-04 punti 1, 2, 3: CAPO VI – Gestione delle emergenze
i) Gestione dell'autenticazione, delle identità digitali e del controllo accessi.	PR.AA-01 punti 1, 2, 3: Art. 9. - Identificazione, autenticazione e autorizzazione e Art. 10. - Registrazione delle attività (Accounting) PR.AA-03 punti 1 e 2: Art. 11. - Corretto uso delle Credenziali di autenticazione e Art. 32. - Accesso remoto (VPN) PR.AA-05 punti 1 e 2: Art. 1. - Principi e Art. 9. - Identificazione, autenticazione e autorizzazione PR.IR-01 punti 1 e 2: Art. 30. - Sistemi di Sicurezza
j) Sicurezza fisica.	PR.AA-06 punto 1: Art. 2. - Ambito di applicazione - Perimetro
k) Formazione del personale e consapevolezza.	PR.AT-01 punti 1, 2 e 3 e PR.AT-02 punti 1 e 2: Regolamento IT
l) Sicurezza dei dati.	PR.DS-01 punti 1 e 2: CAPO II - Strumenti PR.DS-02 punto 1: Art. 20. - Navigazione Internet
m) Sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete.	PR.PS-01: Art. 16. - Sistemi informatici PR.PS-02 punti 1, 2 e 4: Art. 17. - Applicazioni software PR.PS-04 punti 1, 2 e 3: Art. 10. - Registrazione delle attività (*Accounting*)
n) Protezione delle reti e delle comunicazioni.	PR.IR-01 punto 3: Art. 20. - Navigazione Internet e Art. 32. - Accesso remoto (VPN)
o) Monitoraggio degli eventi di sicurezza.	DE.CM-01 punti 1, 4, 5: Art. 30. - Sistemi di Sicurezza, Art. 20. - Navigazione Internet e Art. 10. - Registrazione delle attività (*Accounting*) DE.CM-09 punto 1: Art. 30. - Sistemi di Sicurezza
p) Risposta agli incidenti e ripristino.	RS.MA-01: punto 1: CAPO VI – Gestione delle emergenze