Piano della Sicurezza del Sistema di Conservazione

UNIONE DEI COMUNI GALLURA

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	26/06/2025	Alberto Averini Pisaroni	*R.T.D.*
Verifica	27/06/2025		
Approvazione			

REGISTRO DELLE VERSIONI E RELATIVE DISTRIBUZIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni	Distribuito a
1	26/06/2025	Prima stesura		
2		Seconda stesura		

Sommario

Premessa

All'interno del documento sono indicate tutte le procedure e le metodologie adottate per la gestione, automatizzata e manuale, del sistema informatico della struttura.

Tali procedure nascono dalle indicazioni tecniche fornite nell'ambito delle linee guida per la certificazione ISO/IEC 27001:2013 e le linee guida definite all'interno del Codice dell'Amministrazione Digitale (D.Lgs. 82 del 2005).

Tale piano si pone l'obiettivo di garantire, monitorare e controllare la sicurezza dei sistemi informativi della struttura e, minimizzando il rischio residuo, assicurando la continuità del business e il soddisfacimento dei requisiti relativi alla privacy e alla protezione dei dati personali trattati dall'organizzazione.

Art. 1 – Finalità

Il presente regolamento disciplina:

a) le modalità di accesso ed utilizzo degli strumenti informatici, della rete informatica e dei servizi che tramite la stessa rete è possibile ricevere ed offrire all'interno e all'esterno dell'Amministrazione, nell'ambito dello svolgimento delle proprie mansioni ed attività di ufficio da parte degli amministratori, dei dipendenti e dei collaboratori dell' Unione dei Comuni Gallura;

b) il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione per il trattamento dei dati personali, al fine di garantire l'aderenza e la rispondenza alle vigenti normative in materia, nonché gli adeguati livelli di sicurezza ed integrità del patrimonio informativo dell'Ente;

c) i limiti, i criteri e le modalità per l'utilizzo degli apparecchi cellulari e SIM di proprietà o, comunque, nella disponibilità dell'Ente.

Art. 2 – Ambito di applicazione

1. Il presente regolamento si applica a tutti gli utenti interni (di seguito: utenti) quali gli amministratori, i dipendenti a tempo indeterminato e determinato, il personale assunto con altre forme di rapporto contrattuale, i collaboratori esterni impegnati in attività istituzionali limitatamente al periodo di collaborazione e coloro che, sulla base di specifici rapporti (collaborazioni, incarichi, convenzioni) sono autorizzati ad accedere alle risorse tecnologiche del sistema informatico del Comune o comunque nella disponibilità dell'Ente.

2. Ai fini di quanto previsto nel presente regolamento, verranno di seguito chiamati "Responsabili Informatici" il Segretario/Direttore Generale, per quanto concerne la Segreteria e Direzione Generale e i Responsabili dei servizi o uffici, per quanto concerne le unità organizzative cui sono preposti.

Art. 3 – Principi generali

1. L'Unione dei Comuni Gallura promuove l'utilizzo della rete informatica e telematica, di internet e della posta elettronica quali strumenti utili a perseguire con efficacia ed efficienza le proprie finalità istituzionali, in accordo con le linee guida ed i principi delineati dalla normativa vigente.

2. I dati e le informazioni gestite ed archiviate in modalità informatica costituiscono patrimonio dell'ente, finalizzato all'erogazione di servizi istituzionali. Di conseguenza, allo scopo di consentire la piena disponibilità di tale patrimonio, la gestione informatizzata dei dati deve privilegiare l'utilizzo di sistemi gestionali accentrati, il cui accesso avviene tramite autenticazione fornendo delle credenziali (user-name e password) alle quali viene associato un profilo predeterminato. Nell'ipotesi di gestione con memorizzazione delle informazioni in locale, sul proprio personal computer, l'utente deve provvedere ai salvataggi di sicurezza e, qualora debba assentarsi per ferie o per altri motivi, deve concordare con il proprio Responsabile Informatico le modalità per mettere a disposizione le suddette informazioni.

3. Il Unione dei Comuni Gallura promuove, anche tramite supporti documentali pubblicati nella rete intranet, l'aggiornamento e la formazione dei propri dipendenti sul corretto utilizzo delle strumentazioni informatiche e telematiche.

4. Ogni utente è responsabile, civilmente e penalmente, del corretto uso delle risorse informatiche, dei servizi e dei programmi a cui ha accesso, nonché dei dati trattati a fini istituzionali.

5. Ogni utente è altresì responsabile del contenuto delle comunicazioni effettuate e ricevute a fini istituzionali, anche per quanto attiene la riservatezza dei dati ivi contenuti. Il trattamento dei dati personali deve essere effettuato in conformità alla normativa per la tutela di questi ultimi.

6. L'utilizzo dei cellulari di proprietà o comunque nella disponibilità dell'ente deve avvenire nei soli casi di effettiva necessità e quando le esigenze di servizio lo richiedano.

Art.4 – Criteri di utilizzo delle risorse tecnologiche

Art.4.1 Utilizzo del personal computer

1. Il personal computer è uno strumento di lavoro ed il suo utilizzo deve essere finalizzato esclusivamente allo svolgimento delle attività professionali e istituzionali dell'Amministrazione. Il personal computer viene assegnato all'utente in relazione alle funzioni svolte, previa autorizzazione del Responsabile della struttura di appartenenza. Ciascuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione.

2. Il personal computer assegnato come postazione di lavoro è configurato con il software necessario al suo utilizzo. Ogni ulteriore installazione deve essere concordata con il Responsabile e l'Amministratore di sistema.

3. Ogni utente deve tenere comportamenti corretti, tali da preservare il buon funzionamento degli strumenti e tali da ridurre i rischi per la sicurezza del sistema informatico. E' vietato l'utilizzo di supporti per la memorizzazione dei dati (CD, DVD, memorie USB, etc.) di dubbia provenienza o veicolanti contenuti non inerenti alle esigenze di servizio.

4. E’ necessario spegnere il personal computer al termine dell’attività lavorativa o in caso di assenza prolungata dal proprio ufficio, al fine di evitare l’accesso, anche fortuito, ai dati ivi contenuti, nonché al fine di prevenire utilizzi indebiti da parte di terzi. In presenza di dati personali, anche sensibili, il personal computer dovrà essere bloccato ogniqualvolta rimanga incustodito.

5. Non è consentita l’attivazione della password d’accensione (bios), senza preventiva autorizzazione da parte del Responsabile.

6. I dati archiviati digitalmente devono essere esclusivamente quelli attinenti alle proprie attività lavorative.

7. Costituisce buona regola la pulizia periodica (almeno ogni sei mesi) degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, evitando un’archiviazione ridondante.

8. Ogni utente deve periodicamente verificare che il programma di antivirus sia attivo e funzionante, nonché avviare un controllo antivirus per la verifica sui dischi locali del personal computer a meno che non sia schedulato dall’amministratore di sistema.

9. La tutela dei dati archiviati su personal computer che gestiscono localmente documenti e dati è demandata all’utente, il quale dovrà effettuare periodicamente i salvataggi su supporti dedicati ed idonei, nonché la conservazione degli stessi in luoghi adatti messi a disposizione dall’amministratore di sistema.

10. Non è possibile modificare le configurazioni hardware e software predefinite dagli amministratori di sistema ed installare autonomamente programmi o applicativi senza preventiva autorizzazione.

11. E’ vietata l’installazione, non autorizzata, di sistemi che sfruttino il sistema telefonico o reti wireless per l’accesso a internet o ad altre reti esterne (modem, “chiavette internet”, navigazione tramite cellulare).

12. I sistemisti ed i tecnici di ditte affidatarie del servizio che hanno in gestione le componenti del sistema informatico comunale possono, sentito l’utente, procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza, sia sui singoli personal computer sia sulle cartelle di rete.

13. I sistemisti ed i tecnici incaricati della gestione e della manutenzione del sistema informatico possono altresì, in qualsiasi momento, accedere al personal computer, anche con strumenti di teleassistenza che consentano di operare da remoto sulla postazione dell’utente, per attività di manutenzione preventiva e correttiva, sentito l’utente medesimo.

14. Tutti i dati sensibili riprodotti su supporti esterni (chiavette USB, CD-Rom, DVD) devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato da terzi. Altrettanta cautela deve essere riposta in fase di stampa dei documenti contenenti dati sensibili.

15. L’eventuale malfunzionamento del personal computer e di ogni altra dotazione informatica deve essere tempestivamente comunicato alla ditta affidataria del servizio di assistenza alle attrezzature informatiche.

16. L’eventuale danneggiamento del personal computer e di ogni altra dotazione informatica deve essere tempestivamente segnalato.

17. In caso di furto è onere dell’utente effettuare denuncia all’autorità di polizia.

18. Particolare diligenza deve essere posta dall'utente di PC portatile utilizzato in ambienti esterni all'Amministrazione, sia sotto il profilo della protezione dell'apparecchiatura, sia sotto il profilo della sicurezza dei dati in essa contenuti.

19. È compito di ciascun Responsabile Informatico compartecipare al processo di gestione della sicurezza informatica e collaborare alla verifica del corretto utilizzo delle risorse assegnate, allo scopo di evitarne sia l'uso improprio, sia l'accesso da parte di personale non autorizzato.

20. Nei casi di assegnazione ad altri Settori, Servizi o Uffici dell'ente è compito del dipendente effettuare il passaggio di consegne con la persona individuata dal Responsabile Informatico.

Art.4.2 – Gestione utenti

1. L'abilitazione all'utilizzo delle risorse informatiche dei nuovi dipendenti assunti e di quelli assegnati ad altro Settore o ad altre Unità organizzative fuori settore avverrà su richiesta da parte del Responsabile Informatico della struttura alla quale tali dipendenti sono stati assegnati.

2. Sarà altresì cura del Responsabile Informatico chiedere l'abilitazione all'utilizzo delle risorse informatiche degli stagisti, dei collaboratori esterni o di analoghe figure che operino nell'ambito della struttura cui è preposto, comunicando i dati della persona interessata, nonché le date di inizio e fine dell'account richiesto.

Art. 4.3 – Gestione degli account e delle password

1. L'account è costituito da un codice identificativo personale (username o userid) e da una parola chiave (password).

2. La password che viene associata a ciascun utente è personale, non cedibile e non divulgabile.

3. Le password dovranno avere le seguenti caratteristiche:

- lunghezza minima 8 caratteri;
- caratteri di tipo alfanumerico e contenere almeno un numero, una lettera minuscola e una lettera maiuscola
- contenere almeno un simbolo tipo ? / ! – _ ecc.
- non deve essere riconducibile a:
    - nome o cognome proprio o di un collega o di un famigliare;
    - identificativi di ufficio, di area, di servizio o del Comune, in modo parziale o completo;
    - date di nascita, codici fiscali o altri elementi che ne facilitino l'individuazione.

Art. 4.4 – Utilizzo delle cartelle di rete

1. Le cartelle di rete sono aree di disco su server a disposizione dei vari Settori, Servizi o Uffici. Ogni Settore, Servizio o Ufficio avrà uno spazio la cui dimensione è limitata e determinata, in funzione delle esigenze dei

Settori, Servizi o Uffici, della disponibilità dell'intero sistema di memorizzazione, del numero di utenti, dei volumi e della tipologia di documenti trattati.

2. Le cartelle di rete sono periodicamente salvate con vari metodologie di backup. Le cartelle di rete sono aree di condivisione di documenti strettamente istituzionali e non possono essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia correlato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità.

3. L'organizzazione e la gestione dell'albero delle sottocartelle è demandata ai Responsabili Informatici.

4. L'amministratore di sistema e la ditta affidataria del servizio di assistenza alle attrezzature informatiche, nel caso si prefiguri un uso improprio, o che metta a repentaglio la sicurezza del sistema informatico dell'Ente, delle cartelle di rete, ha la facoltà, di procedere alla rimozione di ogni file o applicazione, nonché di inibire temporaneamente l'accesso alle cartelle di rete interessate.

Art. 4.5– Utilizzo delle stampanti e dei materiali di consumo

L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner, supporti magnetici, supporti digitali) è riservato esclusivamente all'espletamento dei compiti di natura istituzionale. Al fine di conseguire risparmi, devono essere evitati sprechi dei suddetti materiali, in particolare privilegiando soluzioni operative che mirino ad evitare l'utilizzo di carta (memorizzazione di documenti scansionati e comunicazione via mail), nel rispetto delle direttive riguardanti la digitalizzazione della Pubblica Amministrazione.

Art.5 – Gestione delle comunicazioni telematiche

Art. 5.1– Utilizzo di Internet

1. L'utilizzo di Internet deve essere limitato a scopi inerenti l'attività lavorativa.

2. L'Amministrazione adotta misure di filtraggio che permettono di inibire o restringere l'accesso a siti i cui contenuti siano classificati pericolosi o non attinenti agli scopi istituzionali oppure che permettono l'accesso solo a determinati siti la cui consultazione sia stata ritenuta dai singoli Responsabili Informatici utile in relazione agli scopi istituzionali.

3. Sono vietate azioni idonee ad eludere le misure di filtraggio di cui al precedente comma.

4. Nel caso si prefiguri un uso improprio o che metta a repentaglio la sicurezza del sistema informatico dell'ente, il responsabile informatico ha la facoltà di inibire temporaneamente, anche senza preavviso, la navigazione in internet alle postazioni di lavoro interessate.

5. Ai soli fini di gestione e di salvaguardia degli interessi dell'Ente e dei propri dipendenti, il sistema di gestione della navigazione in internet provvede alla tracciatura secondo la normativa vigente, che prevede esclusivamente la registrazione delle URL senza entrare nel merito delle attività svolte (compilazione form, contenuti web-mail, etc). Il tempo di mantenimento di tali dati viene stabilito in 6 mesi, in analogia a quanto previsto nel provvedimento del 24.7.2008 del Garante per la protezione di dati personali.

Art.5.2 – Gestione ed utilizzo della posta elettronica

1. Le caselle di posta elettronica rilasciate sono di due tipi:

– casella di posta elettronica collettiva, riconducibile ad un'unità organizzativa (Settore, Servizio o Ufficio) o ad un gruppo funzionale di utenti che operano all'interno di una stessa unità organizzativa o in più unità organizzative distinte (rientrano in questa tipologia le caselle di posta elettronica certificata);

– casella di posta elettronica individuale, assegnata ad un utente interno.

2. I singoli Responsabili chiedono l'attivazione di caselle di posta elettronica collettive, stabilendo quali utenti vi abbiano accesso, all'amministratore di sistema, avendo cura di comunicare a quest'ultima eventuali variazioni inerenti gli utenti abilitati nonché l'eventuale soppressione della casella stessa.

3. La casella di posta elettronica individuale assegnata ad un utente, nonché quelle collettive cui eventualmente quest'ultimo abbia accesso, sono uno strumento di lavoro ed il loro utilizzo è consentito solo per finalità connesse allo svolgimento della propria attività lavorativa. L'utente è responsabile del loro corretto utilizzo.

4. Non sono consentiti la ricezione o l'invio di messaggi da e verso l'esterno, con allegati di dimensione superiori a 30 Mb e con estensione uguali a .hik .bat .exe .scr ed in generale file di tipo eseguibile o di applicazione. Si precisa che il sistema di sicurezza e antivirus installato a protezione del server di posta elettronica del Unione dei Comuni Gallura non consente la ricezione e l'invio di messaggi di posta che contengono allegati con le caratteristiche sopra descritte. Eventuali esigenze particolari possono essere segnalate alla ditta affidataria del servizio di assistenza alle attrezzature informatiche che provvede ad individuare la soluzione tecnica più appropriata.

5. In caso di inizio o di cessazione del rapporto di lavoro di un dipendente, l'indirizzo di posta elettronica individuale dell'interessato viene attivato o cessato a cura della ditta affidataria del servizio di assistenza alle attrezzature informatiche, su richiesta del Responsabile della struttura cui il singolo dipendente è assegnato.

6. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e con allegati di grandi dimensioni.

7. È vietato utilizzare l'indirizzo delle caselle di posta elettronica collettiva ed individuale per l'invio o la ricezione di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list, salvo autorizzazione del Responsabile Informatico.

8. La conservazione della posta elettronica pervenuta nelle caselle individuali è demandata ad ogni singolo utente. Nel caso in cui i messaggi o allegati debbano essere conservati, l'utente deve autonomamente provvedere al loro salvataggio.

9. La conservazione della posta elettronica pervenuta nelle caselle collettive è demandata ai Responsabili Informatici che hanno richiesto l'attivazione di queste ultime o ai loro delegati.

10. Ai soli fini di gestione e di salvaguardia giuridica degli interessi dell'Ente e dei propri dipendenti, il sistema di gestione della posta elettronica provvede alla tracciatura della corrispondenza in entrata e in uscita, secondo la normativa vigente, che prevede esclusivamente la registrazione dell'identificativo della postazione di lavoro, del mittente e del destinatario. Il tempo di mantenimento di tali dati viene stabilito in

6 mesi, in analogia a quanto previsto nel provvedimento dei 24.7.2008 del Garante per la protezione di dati personali.

Art.6 – Controlli

Art. 6.1 – Controlli e responsabilità

1. L'Amministrazione si riserva di effettuare controlli sul corretto utilizzo degli strumenti informatici e telematici nel rispetto delle normative vigenti in materia di privacy e di tutela della dignità del lavoratore, del presente regolamento e dello Statuto dei lavoratori.

2. Per esigenze organizzative, produttive e di sicurezza l'Amministrazione effettuerà controlli automatizzati generali che avranno carattere anonimo ed avranno ad oggetto dati aggregati, riferiti a Settori, Servizi o Uffici, con l'obiettivo di individuare potenziali rischi per la sicurezza o usi impropri del sistema informatico.

3. Qualora i controlli di cui al precedente comma evidenzino potenziali rischi o problemi oppure nei casi di sospetta violazione delle norme di cui al presente regolamento, l'Amministrazione potrà altresì effettuare controlli e ispezioni su postazioni individuali.

4. Tali controlli ed ispezioni dovranno avvenire con gradualità, nel rispetto dei principi di pertinenza e non eccedenza. I suddetti procedimenti di controllo saranno opportunamente documentati (tipo di controlli, nome del sistemista che opera i controlli, log di accesso ai sistemi, riscontri dei controlli).

5. Il mancato rispetto o la violazione delle norme contenute nel presente regolamento è perseguibile anche in sede disciplinare.

Art.7 – Cellulari, sim di servizio, telefoni fissi e fax

Art.7.1 – Assegnazione

1. I cellulari di servizio di cui al presente capo si suddividono in:

– Cellulari ad uso esclusivo: comprendono i cellulari assegnati in via permanente ed esclusiva al consegnatario in relazione alle funzioni o mansioni svolte;

– Cellulari ad uso non esclusivo: comprendono i cellulari assegnati ad un'unità organizzativa, i quali vengono utilizzati temporaneamente dal personale dell'unità organizzativa stessa, individuato dal responsabile di quest'ultima per il periodo necessario allo svolgimento delle attività che ne richiedono l'uso.

2. I dipendenti comunali possono essere assegnatari di un cellulare di servizio ad uso esclusivo nei seguenti casi:

– per esigenze di reperibilità e servizi fuori sede o assistenza agli impianti;

– frequenti spostamenti tra diverse sedi, anche nella stessa giornata;

– particolari esigenze tecniche di comunicazione di altra natura, tra le quali servizi che non possono essere altrimenti soddisfatti con impianti di telefonia fissa o altri strumenti di comunicazione.

Art. 7.2 – Utilizzo dei cellulari, dei telefoni fissi e del fax

1. Tutti i telefoni cellulari, i telefoni fissi e il fax devono essere utilizzati in modo pertinente alla propria attività lavorativa o carica istituzionale e secondo criteri di effettiva necessità.

2. L'effettuazione delle connessioni dati dell'Ente deve rispondere a criteri di necessità.

3. Al fine di garantire l'immediata rintracciabilità nei casi di necessità, gli utilizzatori dei telefoni cellulari devono mantenere in funzione il telefono cellulare durante le ore di servizio, durante le ore di reperibilità, ove previste, e in tutti i casi in cui le circostanze concrete o il ruolo ricoperto lo rendano opportuno.

4. Ogni assegnatario di apparecchio cellulare è responsabile dell'uso appropriato e della diligente conservazione dell'apparecchio, che non può essere ceduto a colleghi o terzi.

Art. 7.3 – Controlli

L'amministratore di sistema e la ditta affidataria del servizio di assistenza alle attrezzature informatiche per quanto concerne gli aspetti tecnici, effettua controlli sull'utilizzo degli apparecchi cellulari messi a disposizione al fine di verificarne il corretto utilizzo, monitorare e ridurre la spesa.

Il sistema informatico dell'Ente è così costituito:

Infrastruttura su piattaforma virtualizzata presso il CED del Comune di La Maddalena con repliche su cluster presente presso il Palazzo Comunale.

Per maggiori informazioni si veda il Piano di Sicurezza Informatica del Comune di La Maddalena.

Presso la sede dell'Unione dei Comuni troviamo:

- Terminazioni fibra TIM Gigabit con relativi Router;
- Switch di piano per distribuzione rete agli end-point;
- Postazioni client per i dipendenti;
- Stampanti/scanner multifunzione condivise;
- Orologi timbra presenze;
- NAS per la condivisione dei file;

I backup sono programmati a cadenza quotidiana al termine della giornata lavorativa, separati per Settore, su diverse destinazioni: backup primario su VM cloud dedicata allo storage, con copia secondaria su NAS in house.

I computer client e le macchine virtuali sono protetti da soluzione Antivirus con protezione ransomware.

ll personale in smart working utilizza una connessione VPN con credenziali non condivise.

Le varie sedi (Municipio, Palazzo del Sindaco, Ufficio Turismo, Piazza Filigheddu e Centri Sociali/Biblioteca) interconnesse in fibra “Dark Fiber” TIM e ponti Radio della ditta Stel.

Art.8 – Aggiornamenti

Tale piano è soggetto ad aggiornamenti in base all’evoluzione normativa/tecnologica.