
Comune di Saint-Vincent

Regione Autonoma Valle d'Aosta

Région Autonome Vallée d'Aoste



MANUALE DI GESTIONE E CONSERVAZIONE DOCUMENTALE DEL COMUNE DI SAINT-VINCENT

Approvato con deliberazione della Giunta comunale n. 90 del 25/06/2026

Sommario

Parte prima - Disposizioni generali	5
1. Riferimenti normativi	5
2. Finalità e contenuti	5
3. Approvazione e modalità di aggiornamento del Manuale	5
Parte seconda - Organizzazione	6
4. Area organizzativa omogenea (AOO)	6
5. Responsabile della gestione documentale e altri soggetti responsabili	6
6. Sistema informatico di gestione documentale del Comune di Saint-Vincent.....	6
7. Soggetti delegati alle attività di protocollazione del Comune di Saint-Vincent	6
Parte terza - Formazione dei documenti.....	8
Sezione prima: Modalità di formazione.....	8
8. Modalità di formazione dei documenti informatici	8
8.1 Creazione e redazione tramite software di documenti informatici.....	8
8.2 Acquisizione di documenti informatici.....	9
8.3 Copie per immagine su supporto informatico di documenti analogici.....	9
8.4 Duplicati e copie informatici di documenti informatici.....	9
8.5 Acquisizione di istanze tramite servizi online	10
8.5.1 Servizi Fines (Consorzio degli Enti locali della Valle d'Aosta – CELVA).....	10
8.6 Formazione di registri e repertori	10
Sezione seconda: Disposizioni comuni a tutte le modalità di formazione	10
9. Dispositivi di firma elettronica	10
10. Identificazione univoca del documento informatico	10
11. Associazione degli allegati al documento principale	11
12. Accessibilità del documento informatico.....	11
13. Metadati del documento informatico.....	11
14. Immodificabilità ed integrità del documento informatico.....	11
Sezione terza: Disposizioni sulla formazione di documenti analogici	12
15. Copie analogiche di documenti informatici	12
16. Casi in cui è ammessa la formazione di documenti originali analogici.....	12
Parte quarta - Gestione documentale.....	14
Sezione prima - Flussi documentali esterni	14
17. Ricezione telematica di documenti informatici in entrata.....	14
18. Canali di ricezione	14
19. Formati accettati	14
20. Controllo dei certificati di firma	15

21.	Trasmissione telematica di documenti informatici in uscita.....	15
22.	Disposizioni sui documenti analogici	15
	Sezione seconda - Protocollo informatico	16
23.	Sistema di protocollo informatico	16
24.	Funzioni in materia di protocollo informatico	16
25.	Registro generale di protocollo	16
26.	Registro giornaliero di protocollo	16
27.	Documenti soggetti a registrazione di protocollo e documenti esclusi	16
28.	Disposizioni per particolari tipologie di documenti	17
29.	Registrazione di protocollo	17
30.	Modalità di registrazione	18
31.	Annullamento e modifiche della registrazione di protocollo.....	18
32.	Gestione degli allegati	19
33.	Tempi di registrazione e casi di differimento	19
34.	Segnatura di protocollo.....	20
35.	Protocollo riservato.....	20
36.	Registro di emergenza.....	21
37.	Documenti soggetti a registrazione particolare	22
38.	Disposizioni sulla protocollazione di documenti analogici	22
39.1	Registrazione, segnatura, annullamento	23
39.2	Corrispondenza contenente dati sensibili.....	23
39.3	Corrispondenza personale o riservata	23
39.4	Corrispondenza cartacea non di competenza dell'Amministrazione.....	24
	Sezione terza – Classificazione, fascicolazione e accesso ai documenti informatici	24
39.	Classificazione dei documenti	24
40.	Fascicolazione informatica dei documenti.....	24
41.	Accesso ai documenti informatici.....	25
	Sezione quarta – Flussi documentali interni.....	25
42.	Assegnazione dei documenti in entrata agli uffici	25
43.	Comunicazioni interne	25
44.	Pubblicazioni all'Albo pretorio online	26
	Parte quinta – Conservazione dei documenti	27
45.	Sistema di conservazione dei documenti informatici	27
46.	Responsabile della conservazione	27
47.	Oggetti della conservazione	27
48.	Formati ammessi per la conservazione.....	27

49.	Modalità, tempi di trasmissione e gestione dei pacchetti di versamento	28
50.	Memorizzazione dei dati e salvataggio della memoria informatica	28
51.	Accesso al Sistema di conservazione	29
52.	Selezione e scarto dei documenti digitali	29
53.	Conservazione, selezione e scarto dei documenti analogici.....	29
54.	Misure di sicurezza e monitoraggio	29
Parte sesta – Sicurezza e protezione dei dati personali		31
55.	Disposizioni generali	31
56.	Sicurezza dei dati e documenti informatici	31
57.	Protezione dei dati personali: adempimenti in materia	31
58.	Misure organizzative di sicurezza per la protezione e la tutela dei dati nel sistema di gestione informatica dei documenti	32
59.	Registrazione attività rilevanti sul sistema di gestione documentale	33
60.	Amministratore di sistema	33
61.	Uso del profilo utente per l'accesso dei dipendenti ai sistemi informatici	33
62.	Accessibilità da parte degli utenti non appartenenti al Comune di Saint-Vincent	34
63.	Accesso agli archivi analogici del Comune di Saint-Vincent	34

ALLEGATI

Allegato 1.	Riferimenti normativi
Allegato 2.	Glossario
Allegato 3.	Provvedimento di nomina del Responsabile della gestione e conservazione documentale
Allegato 4.	Piano per la sicurezza del sistema di gestione informatica dei documenti
Allegato 5.	Provvedimento di nomina del Responsabile per il trattamento dei dati personali (DPO)
Allegato 6.	Elenco software
Allegato 7.	Manuali software di gestione documentale
Allegato 8.	Formati standard dei documenti informatici
Allegato 9.	Modalità di attestazione delle copie conformi
Allegato 10.	Documento informatico accessibile
Allegato 11.	Titolario di classificazione
Allegato 12.	Registro di protocollo di emergenza
Allegato 13.	Manuale del servizio di conservazione digitale di Maggioli spa
Allegato 14.	Piano di conservazione
Allegato 15.	Modello dei documenti in uscita
Allegato 16.	Manuale utente Servizio di Conservazione Digitale di Maggioli S.p.A.
Allegato 17.	Procedura per la gestione delle abilitazioni di accesso al protocollo informatico
Allegato 18.	Provvedimento di nomina RTD

Parte prima - Disposizioni generali

1. Riferimenti normativi

Il Manuale di gestione e conservazione documentale (d'ora in avanti anche solo "Manuale") del Comune di Saint-Vincent ("Comune" per brevità) è adottato ai sensi delle *Linee guida sulla formazione, gestione e conservazione dei documenti informatici* (d'ora in avanti anche solo "Linee guida"), emanate dall'Agenzia per l'Italia Digitale con determinazione del Direttore generale del 9 settembre 2020, n. 407 e pubblicate il 10 settembre 2020, come modificate dalla determinazione del 17 maggio 2021, n. 371.

Per la normativa di riferimento sulla gestione documentale si rimanda **all'Allegato 1** – Riferimenti normativi, mentre per le definizioni dei termini tecnici si rinvia **all'Allegato 2** - Glossario del Manuale di gestione documentale.

2. Finalità e contenuti

Il presente Manuale, ai sensi del paragrafo 3.5 delle Linee guida, descrive il sistema di gestione informatica dei documenti del Comune di Saint-Vincent e fornisce le istruzioni per la formazione dei documenti informatici, per il corretto funzionamento del servizio, per la tenuta del protocollo informatico, per la gestione dei flussi documentali e degli archivi, ivi compresa la conservazione dei documenti informatici.

Il Manuale presenta un contenuto sia organizzativo che operativo, utile quale strumento di supporto ai processi decisionali e operativi del Comune e, pertanto, è destinato alla più ampia diffusione presso tutto il personale del Comune.

Con la pubblicazione nella sezione "Amministrazione Trasparente" del sito internet istituzionale al seguente link <https://www.comune.saint-vincent.ao.it/documenti/area-amministrativa-generale-e-funzionamento-dell-ente>, il Manuale è reso noto anche esternamente al Comune.

3. Approvazione e modalità di aggiornamento del Manuale

Il presente Manuale e i suoi allegati sono approvati con deliberazione della Giunta Comunale, su proposta dell'Ufficio associato per la transizione al digitale d'intesa con il Responsabile della gestione e conservazione documentale, previo confronto con la Soprintendenza Archivistica e Bibliografica per il Piemonte e la Valle d'Aosta, ai sensi dell'art. 21 del D. Lgs 42/2004 e s.m.i. "*Codice dei beni culturali e del paesaggio*". I successivi aggiornamenti del Manuale, proposti dal Responsabile della gestione documentale, ordinariamente ogni cinque anni, devono essere sottoposti all'approvazione dell'organo competente. ***L'aggiornamento degli allegati, quando non comporta modifiche sostanziali ai contenuti del presente Manuale, è effettuato con determinazione del Segretario comunale, su proposta del Responsabile della gestione documentale.*** Sono da considerarsi modifiche sostanziali quelle aventi a oggetto il Piano di classificazione (Titolario) e il Piano di conservazione dei documenti (Massimario di selezione e scarto).

Parte seconda - Organizzazione

4. Area organizzativa omogenea (AOO)

Il Comune di Saint-Vincent si configura come un'unica Area Organizzativa Omogenea (AOO) denominata UFFICIO PROTOCOLLO (codice IPA del Comune: c_h676; codice univoco dell'AOO: A4D6609).

L'AOO e gli indirizzi di posta elettronica ad essa associati sono indicati nell'indice IPA.

5. Responsabile della gestione documentale e altri soggetti responsabili

Il Comune ha individuato un'unica figura a cui affidare le funzioni e i compiti del Responsabile per la gestione documentale (art. 61 del TUDA) e del Responsabile della conservazione (art. 44, comma 1-quater, del CAD) (**Allegato 3** – Provvedimento di nomina). Poiché non vi sono dirigenti e/o funzionari interni in possesso di idonee competenze giuridiche, informatiche ed archivistiche, il ruolo viene esercitato dal Segretario Comunale.

Il Responsabile della gestione documentale ha i seguenti compiti:

1. gestire i flussi documentali e gli archivi della AOO;
2. provvedere, d'intesa con il Responsabile per la Transizione Digitale – RTD (**Allegato 18** - Provvedimento di nomina), previo parere del Responsabile per la Protezione dei Dati personali – DPO (**Allegato 5** –Provvedimento di nomina), alla predisposizione e al costante aggiornamento del presente Manuale e dei relativi allegati;
3. monitorare i processi e le attività che governano le fasi di formazione, gestione e versamento in conservazione dei documenti informatici;
4. valutare e formulare proposte di riprogettazione e reingegnerizzazione dei processi;
5. vigilare sul rispetto delle norme e delle procedure di produzione e conservazione del registro giornaliero di protocollo;
6. di concerto con l'RTD, effettuare un periodico censimento degli strumenti software di gestione documentale in uso presso il Comune e verificarne la conformità alla normativa vigente.

Ulteriori e specifici compiti del Responsabile sono indicati nelle sezioni pertinenti del presente Manuale. Il Responsabile, ferma restando la propria responsabilità, può delegare in tutto o in parte i propri compiti al personale chiamato eventualmente a collaborare.

6. Sistema informatico di gestione documentale del Comune di Saint-Vincent

Il Sistema informatico di gestione documentale del Comune si avvale delle seguenti soluzioni software (vedi **Allegato 6** - Elenco dei software). La puntuale descrizione delle componenti e delle funzionalità della suite "Sicraweb EVO" è contenuta nel manuale operativo online i cui link sono riportati **nell'Allegato 7** – Manuali software di gestione documentale.

7. Soggetti delegati alle attività di protocollazione del Comune di Saint-Vincent

Il modello di protocollazione adottato dal Comune è parzialmente decentrato. Prevede che siano individuati i dipendenti, all'interno degli uffici, abilitati alla protocollazione informatica dei documenti in uscita e interni. Il Segretario del Comune e i Responsabili di servizio vigilano sul corretto svolgimento delle attività.

La protocollazione dei documenti informatici in entrata è affidata invece, in via esclusiva, al personale addetto dell'Ufficio di protocollo che provvede alla protocollazione dei documenti

pervenuti su supporto cartaceo, dei messaggi e dei documenti pervenuti alle caselle di posta elettronica certificata del Comune, nonché alla protocollazione dei messaggi di posta elettronica ordinaria, secondo le modalità indicate ai paragrafi 29 e ss. del presente Manuale.

BOLLA

Parte terza - Formazione dei documenti

Sezione prima: Modalità di formazione

8. Modalità di formazione dei documenti informatici

Ai sensi del Cap. 2 delle Linee Guida e dell'art. 40 del CAD, tutti i documenti del Comune sono formati in originale come documenti informatici, secondo le modalità individuate all'interno del presente Manuale. La produzione dei documenti è regolata sulla base dei modelli standard resi disponibili dal Comune. I documenti informatici sono formati mediante una delle seguenti modalità:

- produzione tramite l'utilizzo di strumenti di software o servizi cloud qualificati;
- acquisizione della copia per immagine di un documento analogico su supporto informatico (ad esempio, mediante scansione di documento cartaceo);
- acquisizione del duplicato di un documento informatico per via telematica o da supporto informatico;
- memorizzazione su supporto informatico delle informazioni risultanti da transazioni o processi informatici (ad esempio la formazione delle fatture elettroniche tramite SDI);
- generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni secondo una struttura logica predeterminata e memorizzata in forma statica (ad esempio, generazione del registro di protocollo giornaliero).

8.1 Creazione e redazione tramite software di documenti informatici

Gli strumenti software utilizzati dal Comune per la creazione dei documenti informatici sono i programmi della suite Microsoft Office. Il testo del documento informatico creato dagli uffici del Comune, a far data dall'entrata in vigore del presente manuale, deve essere redatto utilizzando esclusivamente font interoperabili "senza grazie" (es. Arial e Times New Roman) di dimensione minima 11. Spaziatura tra paragrafi 0 (zero) e interlinea singola.

Indipendentemente dal supporto con cui sono formati, i documenti del Comune devono garantire la presenza dei seguenti requisiti minimi (v. **Allegato 15** – Modelli dei documenti in uscita):

1. denominazione dell'Amministrazione mediante Logo;
2. autore e ufficio responsabile;
3. oggetto del documento;
4. riferimenti a procedimento;
5. sottoscrizione;
6. data e luogo;
7. numeri di pagina (se in n. superiore a 1);
8. indicazione degli allegati (se presenti);

Se si tratta di un documento in uscita:

1. identificazione e dati dei destinatari;
2. dati dell'Amministrazione (compresi indirizzo e recapiti);
3. mezzo di spedizione.

Il formato del documento informatico deve essere scelto tra i seguenti formati standard: .pdf/A, .xml, o tra quelli indicati per specifici casi nell'Allegato 8 - Tipologie e formati di documenti prodotti e accettati dal Comune al presente Manuale e secondo i criteri ivi stabiliti. Eventuali formati differenti possono essere utilizzati in relazione a specifiche esigenze.

Il formato del documento informatico, in ogni caso, deve essere individuato tra quelli previsti nell'Allegato 2 alle Linee guida dell'AgID, tenendo conto delle raccomandazioni ivi presenti. Le versioni del documento precedenti alla versione definitiva (bozze, etc.) possono essere salvate in un formato che ne consente la modificabilità (ad esempio, .docx o .odt).

La versione definitiva del documento, invece, deve essere sempre in formato PDF/A. I documenti di maggiore rilevanza giuridico-amministrativa prima della firma, devono essere convertiti in formato PDF/A. I documenti in formato PDF/A sono sottoscritti con firma CADES (*.p7m) o, in casi motivati e limitati, con firma PADES. Nel caso il documento definitivo sia di un formato diverso dal PDF/A, la sottoscrizione avviene con firma CADES (*.p7m).

8.2 Acquisizione di documenti informatici

L'acquisizione di documenti informatici può avvenire secondo una delle seguenti modalità:

- acquisizione di un documento informatico per via telematica o su supporto informatico;
- acquisizione della copia per immagine su supporto informatico di un documento analogico (ad esempio, quando si effettua la scansione di un documento cartaceo, memorizzandolo in un formato digitale);
- acquisizione della copia informatica di un documento analogico

In caso di acquisizione di copia informatica del documento originale (analogico o informatico), al fine di assicurarne l'efficacia giuridico-probatoria, occorre attestare la conformità della copia all'originale da cui è estratta (con le modalità indicate nelle disposizioni successive).

In caso di acquisizione di un duplicato informatico ai sensi dell'art. 23-bis del CAD, esso ha la stessa efficacia giuridico-probatoria del documento informatico originale, pertanto non è richiesta l'attestazione di conformità.

8.3 Copie per immagine su supporto informatico di documenti analogici

La copia per immagine su supporto informatico di un documento analogico (ad es. mediante scansione) è prodotta con processi e strumenti che assicurano che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti.

Laddove si debba assicurare la medesima efficacia giuridico-probatoria riconosciuta al documento analogico originale, il dirigente o il funzionario delegato, che agisce in veste di pubblico ufficiale, deve apporre sulla copia informatica del documento, quale risultante dal processo di scansione, l'attestazione di conformità all'originale da cui essa è stata estratta, come indicato **nell'Allegato 9** - Modalità di attestazione di copie conformi.

8.4 Duplicati e copie informatiche di documenti informatici

Un duplicato informatico ha lo stesso valore giuridico del documento informatico da cui è tratto, se è ottenuto mediante la memorizzazione della medesima evidenza informatica. Questa modalità di formazione della copia del documento informatico non necessita di alcuna attestazione di conformità all'originale, perché vi è perfetta coincidenza tra le due evidenze informatiche.

La copia di un documento informatico, invece, è un documento il cui contenuto è il medesimo dell'originale, ma con una diversa evidenza informatica rispetto al documento da cui è tratto (ad es. quando trasformo un documento con estensione '.doc' in un documento '.pdf'). Affinché la copia conservi la medesima efficacia giuridico-probatoria del documento

informatico originale, è necessario attestarne la conformità all'originale come indicato nell'Allegato 9.

8.5 Acquisizione di istanze tramite servizi online

8.5.1 Servizi Fines (Consorzio degli Enti locali della Valle d'Aosta – CELVA)

Le istanze provenienti dai cittadini possono essere formate tramite la compilazione di moduli e form messi a disposizione al link del [servizio di Fines](#) e resi raggiungibili mediante identificazione dell'utente con gli strumenti SPID, CIE e CNS. I dati immessi dall'utente sono acquisiti e memorizzati su supporto informatico. Le istanze così formate sono inviate alla casella PEC del Comune per essere acquisite al sistema di protocollo informatico e costituiscono a tutti gli effetti documenti amministrativi informatici.

8.6 Formazione di registri e repertori

I registri e repertori tenuti dal Comune, compreso il registro giornaliero di protocollo, sono formati mediante la generazione o raggruppamento in via automatica e memorizzazione in forma statica dell'insieme delle registrazioni effettuate dal sistema di gestione documentale.

Sezione seconda: Disposizioni comuni a tutte le modalità di formazione

9. Dispositivi di firma elettronica

Il Comune garantisce che il Segretario e tutti i dipendenti che firmano documenti a valenza esterna siano dotati di dispositivi di firma elettronica. La procedura di acquisto del dispositivo è normalmente a carico del singolo firmatario, in quanto la firma è strettamente personale, ed è in seguito rimborsata dal Comune.

L'utilizzo del dispositivo di firma è strettamente personale e riconducibile al suo titolare. Pertanto, il dispositivo non deve essere ceduto, né devono essere diffuse le chiavi dei certificati.

Ogni titolare di dispositivo di firma verifica periodicamente la validità e la data di scadenza del certificato di firma, al fine di provvedere tempestivamente al rinnovo.

Quando la firma è apposta utilizzando un certificato prossimo alla scadenza (trenta giorni antecedenti la scadenza) il titolare della firma è tenuto ad assicurarsi che venga costituito un riferimento temporale giuridicamente valido tale da attestare che la firma sia stata apposta in un momento in cui il certificato era valido. In particolare, costituisce riferimento temporale giuridicamente valido una delle seguenti attività sul documento firmato:

- apposizione di marca temporale;
- apposizione della segnatura di protocollo;
- versamento in conservazione.

Documenti, dati e altre informazioni trasmesse in cooperazione applicativa con altre PA non richiedono la sottoscrizione digitale (quando è prevista autenticazione applicativa) o l'apposizione della marca temporale.

10. Identificazione univoca del documento informatico

Ogni documento informatico deve essere identificato in modo univoco e persistente. L'identificazione univoca dei documenti è effettuata con l'associazione al documento dell'impronta crittografica HASH. Per i documenti soggetti a registrazione di protocollo,

l'associazione è effettuata tramite le apposite funzioni del sistema di protocollo informatico del Comune. Per i documenti non protocollati, l'associazione è effettuata tramite le apposite funzioni degli strumenti software in uso per la formazione degli atti.

In ogni caso l'impronta crittografica deve essere basata su una funzione di HASH conforme alle tipologie di algoritmi previste **nell'Allegato 6** alle Linee guida (vedi tabella 1 – Digest algorithm del paragrafo 2.2).

11. Associazione degli allegati al documento principale

Gli allegati sono congiunti in modo univoco al documento informatico principale tramite l'associazione delle impronte HASH. Al documento principale, inoltre, vengono essere associati i seguenti metadati:

- numero allegati;
- indice allegati;
- identificativo del documento allegato (IdDoc);
- titolo dell'allegato (Descrizione).

A ciascun allegato, invece, deve essere associato il metadato identificativo del documento principale (IdDoc). Le operazioni di associazione degli allegati, quando possibile, sono effettuate in modo automatizzato dal sistema di gestione documentale utilizzato per la formazione del documento principale. In alternativa, è possibile associare gli allegati al documento principale manualmente, riportando in calce al documento stesso l'elenco degli allegati, indicando per ciascuno l'oggetto e la relativa impronta HASH. L'associazione sarà assicurata una volta che il documento informatico principale sia divenuto imm modificabile (ad esempio, dopo l'apposizione della firma digitale, vedi paragrafo 14 del presente Manuale).

12. Accessibilità del documento informatico

Per garantire l'accessibilità dei documenti informatici alle persone con disabilità, anche ai fini della pubblicazione e dell'accesso documentale, i soggetti responsabili della formazione del documento seguono le indicazioni contenute nella "Guida pratica per la creazione di un documento accessibile" di cui **all'Allegato 10** – Documento informatico accessibile al presente Manuale.

13. Metadati del documento informatico

Al documento informatico e al documento amministrativo informatico devono essere associati i metadati obbligatori previsti dall'Allegato 5 alle Linee guida dell'AgID. Ulteriori metadati facoltativi sono associati secondo le indicazioni riportate **nell'Allegato 8** al presente Manuale. I metadati devono essere associati prima che il documento informatico acquisisca le caratteristiche di imm modificabilità e integrità, dunque prima della sottoscrizione, della memorizzazione nel sistema o del versamento in conservazione.

14. Immodificabilità ed integrità del documento informatico

Per garantire il valore giuridico e probatorio di un documento informatico, è necessario assicurare la sua imm modificabilità e integrità.

Un documento informatico è imm modificabile se, durante le fasi di accesso, gestione e conservazione, la sua memorizzazione su supporto digitale non può essere alterata.

L'immodificabilità e l'integrità dei documenti informatici del Comune sono garantite attraverso diverse modalità:

- per i documenti che richiedono la sottoscrizione: l'apposizione di una firma elettronica qualificata, una firma digitale, un sigillo elettronico qualificato o una firma elettronica avanzata.
- per i documenti che non richiedono sottoscrizione: la loro memorizzazione all'interno di un sistema di gestione documentale, a condizione che siano rispettate le misure di sicurezza stabilite (vedi la Parte Sesta del presente Manuale).
- per tutte le tipologie documentali: il versamento nel sistema di conservazione documentale.

Il versamento nel sistema di conservazione rappresenta la soluzione che offre le più alte garanzie di immodificabilità e integrità dei documenti nel tempo. Pertanto, è fondamentale che tutti i documenti destinati alla conservazione vengano correttamente versati nel sistema di conservazione elettronica, secondo le modalità e i tempi descritti nella Parte Quinta del presente Manuale.

Sezione terza: Disposizioni sulla formazione di documenti analogici

15. Copie analogiche di documenti informatici

Noto l'obbligo di creare i documenti originali informatici, talvolta vi è la necessità di effettuare delle copie analogiche affinché siano spedite a mezzo posta ai soggetti che non sono muniti di domicilio digitale e agli altri soggetti indicati all'art. 3-bis, comma 4-bis, del CAD.

Quando è necessario che al destinatario giunga un documento avente la medesima efficacia giuridico-probatoria del documento originale (ad esempio, quando bisogna assicurare l'efficacia legale della notificazione dell'avviso di accertamento relativo a tributi o a violazioni da cui discendono sanzioni amministrative), ai sensi dell'art. 3, D.lgs. n. 39/1993, la copia analogica dovrà essere accompagnata dall'indicazione della fonte del documento originale e del soggetto responsabile dell'immissione, riproduzione, trasmissione o emanazione del documento stesso.

Quando il documento originale informatico è sottoscritto con firma digitale o altra firma elettronica qualificata, la firma è sostituita dall'indicazione a stampa del nominativo del soggetto responsabile.

La copia analogica inviata al cittadino, inoltre, deve contenere apposita dicitura che specifichi che il documento informatico, da cui la copia è tratta, è stato predisposto come documento nativo digitale ed è disponibile presso l'amministrazione (ad es.: *"COPIA CONFORME ALL'ORIGINALE INFORMATICO. (Art.20 D.P.R. 445/2000 Art.23 D.lgs. 07 marzo 2005 n.82, e ss.mm.ii.) La presente copia cartacea è conforme all'originale informatico, sottoscritto con firma digitale, il cui certificato intestato a [NOME e COGNOME] è valido e non revocato, e la cui verifica ha avuto esito positivo. Documento stampato il giorno [DATA]. FIRMATO [NOME e COGNOME] Impronta HASH (SHA256) [tipologia prevista dalle Linee Guida Agid]"*).

16. Casi in cui è ammessa la formazione di documenti originali analogici

Fermo restando l'obbligo di produrre i propri documenti in originale informatico, è legittimo formare documenti in originale analogico:

- ai sensi dell'art. 2, comma 6, del CAD, esclusivamente nell'ambito dell'esercizio di attività e funzioni di ordine e sicurezza pubblica, difesa e sicurezza nazionale, polizia giudiziaria e polizia economico-finanziaria e consultazioni elettorali, nonché alle comunicazioni di emergenza e di allerta in ambito di protezione civile;

- in tutti i casi in cui il documento è consegnato a sportello e il richiedente è un soggetto privato che non agisce in qualità di impresa o professionista.

BOLLA

Parte quarta - Gestione documentale

Sezione prima - Flussi documentali esterni

17. Ricezione telematica di documenti informatici in entrata

I documenti informatici in entrata, pervenuti tramite i canali di ricezione previsti, sono oggetto di registrazione di protocollo secondo quanto previsto nella Sezione seconda della presente Parte del Manuale. Una volta che ne sia accertata la provenienza, i documenti sono validi ai fini del procedimento amministrativo.

Le istanze, le dichiarazioni e le comunicazioni trasmesse per via telematica, in ogni caso, devono ritenersi valide a tutti gli effetti di legge quando:

1. sono contenute in documenti sottoscritti con firma digitale o firma elettronica qualificata;
2. sono trasmesse a mezzo posta elettronica certificata da un indirizzo PEC iscritto in uno degli elenchi di domicili digitali previsti dalla normativa vigente;
3. sono trasmesse attraverso un sistema informatico che consente la previa identificazione dell'utente con i sistemi SPID, CIE, CNS o eIDAS;
4. sono trasmesse da un domicilio digitale ai sensi dell'art. 3-bis, comma 4- quinquies, del CAD ed è possibile accertare la provenienza della trasmissione. Tale modalità di trasmissione costituisce elezione di domicilio digitale speciale per quel singolo procedimento o affare;
5. sono contenute in copie digitali di documenti originali cartacei sottoscritti e presentati unitamente a copia del documento d'identità dell'autore;
6. è comunque possibile accertarne la provenienza secondo la normativa vigente o, comunque, in base a criteri di attendibilità e riconducibilità al mittente dichiarato.

18. Canali di ricezione

La ricezione delle comunicazioni e dei documenti informatici è assicurata tramite i seguenti canali:

- Casella PEC: protocollo@pec.comune.saint-vincent.ao.it
- Canali di trasmissione come posta elettronica ordinaria indicati per specifici procedimenti.

Qualora un soggetto, tenuto ad effettuare comunicazioni esclusivamente in via telematica (imprese, professionisti, altre Pubbliche amministrazioni, salvi i casi di cui all'art. 2, co.6 del CAD) faccia pervenire agli uffici del Comune comunicazioni e documenti in modalità analogica, questi non saranno ritenuti validamente trasmessi. In questi casi, la situazione è segnalata in nota alla registrazione di protocollo.

Il soggetto individuato quale responsabile del procedimento, ai sensi dell'art. 5, comma 3, l. n. 241/1990 o dell'art. 8 della l.r. n. 19/2007, provvede a comunicare al mittente il motivo della mancata accettazione dei documenti e a indicare modalità di trasmissione valide. La comunicazione, quando possibile, è trasmessa al domicilio digitale del mittente estratto dagli indici di cui agli articoli 6-bis e 6-ter del CAD.

19. Formati accettati

Sono accettati, e conseguentemente registrati al protocollo, documenti informatici esclusivamente nei formati previsti **dall'Allegato 8**.

Il controllo sulla conformità del formato dei documenti in entrata è effettuato dal personale addetto alla protocollazione prima della registrazione di protocollo. Qualora pervengano documenti in formati non ammessi e si provveda comunque alla protocollazione, la circostanza deve essere indicata in nota al momento della registrazione di protocollo e segnalata al responsabile del procedimento, affinché ne dia comunicazione al mittente.

A seconda della tipologia di procedimento, il Responsabile del procedimento può limitare le tipologie di formati accettati, purché le limitazioni siano ragionevoli e giustificate da obiettive esigenze legate al procedimento. Il Responsabile del procedimento verifica il formato dei documenti ricevuti e comunica al mittente l'eventuale non conformità del documento e/o l'assenza dei requisiti previsti. L'accettazione di formati non previsti dalle Linee Guida o dalla disciplina del singolo procedimento deve essere consentita nel caso in cui, per esigenze rappresentate dal mittente, il documento non può essere riversato in altro formato tra quelli ammessi.

20. Controllo dei certificati di firma

Il Responsabile del procedimento e/o dell'istruttoria verifica la validità dei certificati di firma e, in caso di certificato scaduto o revocato, lo segnala al personale addetto alla protocollazione, affinché indichi la circostanza in nota alla registrazione di protocollo (v. procedura di modifica di cui all'art. 31 del Manuale). Il Responsabile del procedimento e/o dell'istruttoria, inoltre, valuta le azioni da intraprendere a seconda della tipologia di procedimento.

21. Trasmissione telematica di documenti informatici in uscita

La trasmissione di comunicazioni e documenti avviene sempre per via telematica, eccetto in caso di trasmissione a soggetti privati privi di domicilio digitale, ai sensi degli artt. 6 e ss. del CAD.

Per la trasmissione telematica di documenti a imprese e professionisti, i quali sono tenuti per legge all'iscrizione in albi o elenchi, il domicilio digitale è estratto dall'indice [INI-PEC](#).

Per la trasmissione telematica di documenti a privati cittadini, qualora siano in possesso di domicilio digitale, è ricavato, ove possibile, dall'[indice INAD](#). La consultazione dell'indice INAD è obbligatoria prima dell'invio.

I documenti informatici in uscita sono trasmessi a mezzo PEC solo dopo essere stati classificati e protocollati secondo le disposizioni della presente Parte del Manuale.

La trasmissione di comunicazioni e documenti verso altre pubbliche amministrazioni avviene sempre per via telematica. Gli indirizzi di spedizione sono rilevati tramite la consultazione dell'[Indice delle Pubbliche Amministrazioni](#) di cui all'art. 6-ter del CAD.

22. Disposizioni sui documenti analogici

I documenti su supporto analogico possono pervenire al Comune tramite:

- il servizio postale;
- la consegna diretta agli uffici agli addetti alle attività di sportello;

Gli orari definiti per la presentazione della documentazione analogica sono indicati sul sito web istituzionale del Comune <https://www.comune.saint-vincent.ao.it>

Le buste delle comunicazioni cartacee pervenute tramite raccomandata sono conservate insieme ai documenti in esse contenuti.

Sezione seconda - Protocollo informatico

23. Sistema di protocollo informatico

Il Comune, per la protocollazione dei documenti, utilizza un apposito sistema di protocollo informatico. La descrizione funzionale e operativa del sistema di protocollo informatico è illustrata nel manuale di utilizzo di cui **all'Allegato 7**.

24. Funzioni in materia di protocollo informatico

Presso il Comune la corretta tenuta del protocollo informatico è garantita dal funzionario responsabile del servizio amministrativo, nella veste di responsabile del protocollo informatico:

- coordina la gestione del sistema di protocollo informatico;
- assicura la corretta esecuzione delle attività di protocollazione;
- autorizza l'attivazione del protocollo di emergenza e il successivo ripristino del protocollo informatico;
- autorizza le operazioni di annullamento delle registrazioni di protocollo;
- in collaborazione con il Responsabile della Gestione documentale vigila sull'osservanza della normativa e delle disposizioni del presente Manuale da parte del personale addetto.

Le attività di protocollazione sono eseguite dagli utenti autorizzati. La modalità di individuazione dei soggetti autorizzati alle attività di protocollazione è definita all' art. 7 del presente Manuale.

25. Registro generale di protocollo

Nell'ambito della AOO, il Registro generale di protocollo è unico, al pari della numerazione progressiva delle registrazioni di protocollo.

Il numero di protocollo è costituito da almeno sette cifre numeriche.

La numerazione è progressiva, si chiude al 31 dicembre di ogni anno e ricomincia dal primo gennaio dell'anno successivo.

Il numero di protocollo e la data di protocollo sono generati tramite il sistema di protocollo informatico ed assegnati automaticamente a ciascun documento registrato. Non è consentita la protocollazione di un documento già protocollato.

26. Registro giornaliero di protocollo

Il registro giornaliero di protocollo è costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno. Esso è prodotto automaticamente dal sistema di protocollo informatico, che provvede altresì al versamento automatico al Sistema di conservazione.

27. Documenti soggetti a registrazione di protocollo e documenti esclusi

Tutti i documenti prodotti e ricevuti dal Comune, indipendentemente dal supporto sul quale sono formati, sono registrati al protocollo.

I documenti interni di preminente carattere giuridico-probatorio sono quelli redatti dal personale nell'esercizio delle proprie funzioni e al fine di documentare fatti inerenti all'attività

svolta e alla regolarità delle azioni amministrative o comunque qualsiasi altro documento dal quale possano nascere diritti, doveri o legittime aspettative di terzi.

Essi sono soggetti alla registrazione di protocollo che, attestandone il momento della consegna da un servizio ad un altro o tra gli organi o tra organi e servizio, ne definisce contestualmente il trasferimento di responsabilità in relazione al procedimento o all'affare di cui fanno parte o che viene contestualmente attivato.

I documenti interni di preminente carattere informativo, invece, sono di norma documenti di lavoro di natura temporanea che possono non entrare a far parte del fascicolo definitivo relativo all'affare di cui trattano: memorie informali, appunti, bozze di documenti prive di annotazioni significative, brevi comunicazioni di rilevanza meramente informativa. Non sono soggetti a protocollo e la loro circolazione avviene tramite semplice consegna all'ufficio destinatario tramite posta elettronica.

Sono altresì esclusi dalla protocollazione, ai sensi dell'articolo 53 del TUDA:

- Gazzette Ufficiali, Bollettini Ufficiali, notiziari della Pubblica Amministrazione;
- note di ricezione delle circolari e altre disposizioni;
- materiale statistico;
- atti preparatori interni;
- giornali, riviste, materiale pubblicitario, stampe varie, plichi di libri;
- biglietti augurali, inviti a manifestazioni e documenti di occasione vari che non attivino procedimenti amministrativi;
- bolle accompagnatorie;
- richiesta/invio comunicazioni informali.

28. Disposizioni per particolari tipologie di documenti

La protocollazione della documentazione di gara e delle offerte, scaricabili dalle piattaforme e-procurement dei mercati elettronici della Pubblica Amministrazione, della Regione o da altre piattaforme conformi alla normativa vigente, non è necessaria quando i gestori di tali sistemi assicurano la conservazione a tempo indeterminato della documentazione relativa alle singole gare. In tali casi si ritiene comunque opportuno protocollare la richiesta d'offerta o dell'ordine diretto di acquisto e l'offerta dell'impresa aggiudicataria acquisendo, per questa, tutti i documenti relativi e specificando, negli appositi campi o nelle note, data e ora di arrivo.

29. Registrazione di protocollo

La registrazione di protocollo è l'insieme delle informazioni (metadati) che il registro di protocollo deve memorizzare in forma non modificabile al fine di garantirne l'identificazione univoca e certa. Ai sensi dell'art. 53, comma 1, del TUDA, i dati di registrazione di protocollo sono:

1. numero di protocollo del documento, generato automaticamente dal sistema e non modificabile;
2. data di registrazione di protocollo, assegnata automaticamente dal sistema e non modificabile;
3. il mittente, per i documenti ricevuti, e il destinatario (o i destinatari), per i documenti inviati;
4. oggetto del documento;
5. data e numero di protocollo del documento ricevuto, se disponibili;
6. l'impronta del documento informatico;
7. classificazione (titolo e classe) sulla base del Titolario (**Allegato 11**);

8. assegnazione interna (per competenza o per conoscenza).

Ai dati registrati in forma non modificabile, inoltre, possono essere aggiunti (a seconda dei casi) le seguenti ulteriori informazioni:

1. tipologia di documento;
2. data e ora di arrivo;
3. allegati;
4. livello di riservatezza;
5. mezzo di ricezione o invio;
6. annotazioni;
7. (eventualmente) estremi del provvedimento di differimento della registrazione;
8. (se necessario) elementi identificativi del procedimento amministrativo.

30. Modalità di registrazione

La registrazione di protocollo di un documento è eseguita dopo averne verificato l'autenticità, la provenienza e l'integrità.

La registrazione dei documenti ricevuti, spediti e interni è effettuata in un'unica operazione, utilizzando le apposite funzioni previste dal sistema di protocollo informatico. Al documento indirizzato a più destinatari deve essere assegnato un solo e unico numero di protocollo.

Il sistema genera automaticamente il numero progressivo e la data di protocollazione associata. Alla registrazione di protocollo, inoltre, sono associate le ricevute generate dal sistema di protocollo informatico. Le ricevute di accettazione e di consegna di un messaggio inviato tramite PEC non devono essere protocollate, ma devono essere associate alla registrazione di protocollo del documento trasmesso/ricevuto a cui la ricevuta stessa si riferisce.

L'eventuale indicazione dell'ufficio (assegnazione interna), ovvero del soggetto destinatario del documento, va riportata nella registrazione di protocollo.

Gli utenti non abilitati alla protocollazione in entrata, per la protocollazione della posta elettronica ordinaria, provvedono a inoltrare il messaggio in entrata all'indirizzo di posta ordinaria del Servizio di Protocollo (info@comune.saint-vincent.ao.it) inserendo nel testo della trasmissione la seguente dicitura "SI PREGA DI PROTOCOLLARE". In questi casi, dunque, l'utente addetto al protocollo provvede alla protocollazione del messaggio inoltrato, assicurandosi che siano registrati i relativi dati.

31. Annullamento e modifiche della registrazione di protocollo

La registrazione degli elementi obbligatori del protocollo non può essere modificata, integrata o cancellata, ma soltanto annullata attraverso l'apposita procedura conforme all'art. 54 del TUDA. In particolare, i dati indicati all'art. 29 del presente Manuale, da 1) a 8), non sono modificabili, ma eventualmente annullabili.

Ogni annullamento della registrazione deve:

- essere autorizzato dal Responsabile del protocollo (funzionario Responsabile del servizio amministrativo) o suo delegato;
- assicurare la memorizzazione di data, ora e estremi dell'operazione di annullamento;
- prevedere la memorizzazione e la visibilità delle informazioni oggetto di annullamento.

Le richieste di annullamento rivolte al Responsabile del protocollo devono essere motivate. Le richieste sono accolte, di norma, in casi di mero errore materiale (quali ad esempio la doppia registrazione, la registrazione di documenti che non diano seguito a procedimenti o

ad attività amministrative proprie del Comune, la registrazione errata che necessiterebbe di modifiche sostanziali dei campi obbligatori).

Solo il Responsabile del protocollo ha il potere di autorizzare l'annullamento delle registrazioni di protocollo, ovvero di dare disposizioni in tal senso. Il Responsabile del protocollo può delegare il personale addetto al Servizio di Protocollo ad autorizzare le operazioni di annullamento, che devono risultare in modo esplicito nel provvedimento di delega. In tal caso, la comunicazione formale di autorizzazione resa dal delegato deve indicare gli estremi del provvedimento di delega.

Come previsto dal par. 3.1.5. delle Linee Guida AgID, le uniche informazioni modificabili di una registrazione di protocollo sono quelle relative a:

- classificazione (titolo e classe);
- assegnazione interna all'amministrazione (per competenza o per conoscenza).

Le operazioni di modifica possono essere svolte dal personale addetto alla protocollazione, anche senza previa autorizzazione del Responsabile del protocollo.

L'annullamento e le modifiche avvengono secondo la procedura guidata dal sistema (vedi **Allegato 7**), che consente di mantenere traccia di ogni operazione (tracciamento e storicizzazione), così come richiesto alla normativa.

32. Gestione degli allegati

Il numero e la descrizione degli allegati sono elementi essenziali per l'efficacia di una registrazione. Tutti gli allegati devono pervenire con il documento principale al fine di essere inseriti nel sistema di protocollo informatico ed essere sottoposti a registrazione.

Gli allegati dei documenti ricevuti tramite il canale PEC sono gestiti in forma automatizzata dal sistema di protocollo informatico. Negli altri casi, l'associazione degli allegati al documento principale avviene con le modalità indicate all' art. 11 del presente Manuale.

Non è ammessa l'associazione al documento informatico già registrato di allegati non indicati nella registrazione di protocollo.

33. Tempi di registrazione e casi di differimento

La registrazione della documentazione in entrata deve avvenire in giornata o comunque non oltre il giorno lavorativo successivo a quello di arrivo. Ai fini della gestione del protocollo non sono considerati lavorativi il sabato e la domenica.

In casi eccezionali ed imprevisti che non permettono di evadere la corrispondenza ricevuta e, qualora dalla mancata registrazione di protocollo del documento nella medesima giornata lavorativa di ricezione possa venire meno un diritto di terzi (ad esempio per la registrazione di un consistente numero di domande di partecipazione ad un concorso in scadenza), con motivato provvedimento del Responsabile del protocollo è autorizzato il differimento dei termini di registrazione (protocollo differito).

Il protocollo differito si applica solo ai documenti in entrata e per tipologie omogenee che il Responsabile del protocollo deve descrivere nel provvedimento. Il provvedimento individua i documenti da ammettere alla registrazione differita, le cause e il termine entro il quale la registrazione di protocollo deve essere comunque effettuata.

Al momento della registrazione differita devono essere indicati in nota alla registrazione gli estremi del provvedimento di differimento. In ogni caso, della ricezione del documento

informatico da parte del Comune, fa fede la ricevuta di consegna generata dal gestore della casella PEC.

Ai fini del computo di termini previsti dalla legge o da altri atti (es. bandi, contratti, etc.), resta fermo quanto previsto dall'art. 45, comma 2, del CAD, ai sensi del quale il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore.

34. Segnatura di protocollo

La segnatura di protocollo è l'associazione ai documenti amministrativi informatici in forma permanente e non modificabile di informazioni riguardanti i documenti stessi, in ingresso e in uscita al sistema di protocollo, utile alla sua identificazione univoca e certa, come indicato all'art. 53, comma 1, del TUDA.

Le operazioni di segnatura sono effettuate contemporaneamente alla registrazione di protocollo o ad altra registrazione cui il documento è soggetto.

I requisiti necessari di ciascuna segnatura di protocollo sono:

1. indicazione della Amministrazione;
2. codice identificativo dell'AOO;
3. codice identificativo del registro;
4. numero progressivo di protocollo;
5. data di registrazione;
6. oggetto del documento;
7. classificazione archivistica;
8. eventuale indicazione del fascicolo in cui è inserito il documento.

Per i documenti informatici trasmessi ad altre Pubbliche Amministrazioni, i dati relativi alla segnatura di protocollo sono contenuti, un'unica volta nell'ambito dello stesso messaggio, in un file XML conforme alle indicazioni previste al paragrafo 2 e seguenti dell'Allegato 6 alle Linee guida dell'AgID e, in particolare, devono rispettare lo schema di cui al paragrafo 4 - Appendice A intitolata XML – Schema della segnatura di protocollo, con particolare riguardo al paragrafo 4.1. "Segnatura di protocollo XML Schema".

35. Protocollo riservato

Possono essere previste particolari forme di riservatezza e di accesso controllato al sistema di protocollo per:

- documenti contenenti categorie particolari di dati personali ai sensi dell'art. 9 del Regolamento UE 2016/679 che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (ad es. documenti che contengono certificati medici con diagnosi o patologie, certificati di invalidità, documenti attestanti l'adesione a partiti politici, documenti contenenti sfratti esecutivi e pignoramenti, ecc.), dati personali relativi a condanne penali e reati o a connesse misure di sicurezza;
- documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, potrebbero ostacolare il raggiungimento degli obiettivi prefissati o procurare

pregiudizio a terzi o al buon andamento dell'attività amministrativa (tipologie documentarie definite all'art. 24 della legge n. 241/1990);

- segnalazioni indirizzate al Responsabile della prevenzione della corruzione e della trasparenza, che nel Comune è il Segretario, ai sensi della normativa in materia di whistleblowing.

I documenti registrati con tali forme appartengono al protocollo riservato del Comune, costituito dalle registrazioni sul Sistema di protocollo il cui accesso è consentito solamente agli utenti autorizzati.

Le tipologie di documenti da registrare nel protocollo riservato sono codificate all'interno del sistema di protocollo informatico a cura del Responsabile del protocollo.

36. Registro di emergenza

Il registro di protocollo informatico può, in condizioni di emergenza, non essere disponibile.

Per garantire la normale attività di protocollazione in entrata e in uscita il Responsabile della gestione documentale autorizza lo svolgimento delle operazioni di protocollo sul registro di emergenza.

Il Comune è provvisto di registro di protocollo di emergenza sia informatico sia cartaceo da attivarsi in base alle diverse problematiche che si possono presentare. Il Responsabile del protocollo provvede alla formazione del registro di emergenza su foglio di calcolo o, a seconda del guasto, su supporto analogico, redatto secondo lo schema di cui **all'Allegato 12**.

L'attivazione del registro di protocollo di emergenza avviene se si verificano tre condizioni, non necessariamente dipendenti l'una dall'altra:

1. guasto al software del protocollo
2. guasto al sistema informatico di gestione
3. mancanza di energia elettrica

Per l'attivazione del registro di protocollo di emergenza è necessario:

1. redigere il verbale di attivazione del registro;
2. compilare il registro di protocollo di emergenza;
3. dare comunicazione agli Uffici del Comune dell'attivazione dell'emergenza.

L'utilizzo del registro di protocollo di emergenza, ai sensi dell'art. 63 del TUDA, è autorizzato dal Responsabile del protocollo, o in assenza dal suo delegato, in situazioni nelle quali per cause tecniche non sia possibile utilizzare il registro generale di protocollo informatico e la sospensione del servizio si protragga per un tempo tale da poter pregiudicare la registrazione a protocollo in giornata. In tali casi, il Responsabile del protocollo dà immediata comunicazione a tutti gli uffici della temporanea sospensione dell'utilizzo della procedura informatizzata ordinaria di protocollazione e della necessità, per la protocollazione in entrata, in uscita e interna, di consegnare la documentazione all'Ufficio protocollo.

Il registro di protocollo di emergenza ha una numerazione progressiva propria, perciò ai documenti protocollati su tale registro, una volta riversati, saranno associati due numeri di protocollo, quello del registro di emergenza e quello del registro di protocollo generale. Ad ogni registrazione recuperata dal registro di emergenza viene attribuito un nuovo numero di protocollo effettivo e la data di registrazione, seguendo senza soluzione di continuità la numerazione del protocollo effettivo, ossia la numerazione del protocollo unico raggiunta al momento dell'interruzione del servizio.

Le registrazioni sul registro di emergenza avvengono, quando possibile, secondo le medesime regole e con le stesse modalità adoperate per le registrazioni sul registro generale di protocollo.

Sul registro di emergenza, inoltre, sono riportati:

- gli estremi del provvedimento di autorizzazione all'utilizzo del registro;
- la causa, la data e l'ora di inizio dell'interruzione;
- il numero totale di registrazioni effettuate nel corso di ogni giornata di utilizzo;
- la data e l'ora del ripristino della funzionalità del sistema;
- ogni altra annotazione ritenuta rilevante.

Al ripristino della piena funzionalità del sistema di protocollo informatico, il Responsabile del protocollo provvede alla chiusura del registro di emergenza, annotando il numero delle registrazioni effettuate, la data e l'ora di chiusura, e dà disposizioni per il riversamento delle registrazioni sul registro di protocollo generale. Nel registro di emergenza la numerazione va da 1 a n all'interno dell'anno solare, pertanto in caso di 2 utilizzi nello stesso anno solare le registrazioni del secondo evento di emergenza riprenderanno la numerazione dall'ultima registrazione del primo evento. Il registro di emergenza è destinato alla conservazione permanente.

37. Documenti soggetti a registrazione particolare

La registrazione particolare dei documenti richiede lo svolgimento delle medesime operazioni di gestione documentale effettuate per la registrazione di protocollo, ivi incluse la classificazione e la eventuale fascicolazione (se presente).

Sono soggette a registrazione particolare, nei repertori e registri istituiti, le tipologie di documenti di seguito riportate:

- Deliberazioni della Giunta;
- Deliberazioni del Consiglio;
- Decreti del Sindaco;
- Determinazioni (incluse le determinazioni di liquidazione);
- Ordinanze;
- Contratti soggetti a repertorio.

I registri e repertori diversi dal protocollo contengono almeno le seguenti informazioni:

- tipologia del registro o repertorio;
- numero di registro o repertorio (cronologico e progressivo);
- data;
- elementi identificativi dell'atto (soggetto o soggetti; oggetto);
- dati di classificazione;
- annotazioni.

Al fine di garantire i medesimi effetti della registrazione di protocollo, i registri e repertori di cui al presente paragrafo sono conservati con modalità analoghe a quelle del registro giornaliero di protocollo informatico.

38. Disposizioni sulla protocollazione di documenti analogici

Il personale dell'Ufficio protocollo, addetto ad effettuare la registrazione di protocollo informatica in entrata, è competente anche per la protocollazione dei documenti analogici in entrata (consegnati a mano o pervenuti tramite servizio postale). Di tale documentazione è

effettuata una copia per immagine su supporto informatico (scansione in formato pdf) dopo la registrazione.

La copia per immagine di documenti firmati, se sprovvista di attestazione di conformità, apposta ai sensi della normativa vigente (v. le procedure definite al par. 8.4 del presente Manuale), può essere adoperata per uso interno e non rappresenta la dematerializzazione del documento analogico, il quale è destinato alla conservazione.

Qualora il documento analogico sia consegnato direttamente dal mittente o da altra persona a ciò delegata e sia richiesto il rilascio di una ricevuta attestante l'avvenuta consegna del documento, è cura del personale addetto rilasciare la ricevuta di avvenuta protocollazione prodotta direttamente dal protocollo informatico.

Qualora per ragioni organizzative o tecniche non sia possibile protocollare immediatamente il documento, l'addetto al protocollo comunica al mittente o ad altra persona incaricata il termine entro il quale il documento verrà protocollato, impegnandosi, se richiesto, a far pervenire la ricevuta all'indirizzo e-mail indicato dal mittente stesso. La ricevuta può essere altresì ritirata dall'interessato o da persona espressamente delegata nei giorni successivi.

La ricevuta di avvenuta protocollazione prodotta dal sistema di protocollo riporta i seguenti dati:

- il numero e la data di registrazione;
- l'indicazione dell'AOO;
- l'oggetto;

39.1 Registrazione, segnatura, annullamento

Alla registrazione di protocollo dei documenti cartacei si applicano, in quanto compatibili, le medesime regole previste per la registrazione dei documenti informatici.

Le lettere anonime sono soggette a registrazione di protocollo, eventualmente riservato, indicando nel campo del mittente la dicitura "Anonimo".

Per i documenti analogici la segnatura è apposta con un timbro riportante i seguenti dati:

- Nome dell'Amministrazione: Comune di Saint-Vincent;
- numero progressivo di protocollo;
- data di registrazione;
- classificazione archivistica.

Sul documento analogico soggetto ad annullamento della registrazione si deve riportare a margine il numero di protocollo e la data dell'autorizzazione di annullamento. La segnatura (timbro) deve essere barrata con la dicitura "*annullato*".

39.2 Corrispondenza contenente dati sensibili

I documenti contenenti categorie particolari di dati o soggetti a riservatezza, pervenuti in modalità cartacea, dopo essere stati scansionati e allegati alla registrazione effettuata con protocollo, devono essere inseriti in busta chiusa recante la dicitura "contiene dati sensibili" e successivamente consegnati al funzionario competente in base all'assegnazione.

39.3 Corrispondenza personale o riservata

La corrispondenza nominativamente intestata è regolarmente aperta dagli uffici incaricati della registrazione di protocollo dei documenti in arrivo. Se la corrispondenza riveste carattere "riservato" o "personale", e ciò è desumibile prima dell'apertura della busta, questa

viene inviata chiusa direttamente al destinatario priva di registrazione. Se il carattere “riservato” o “personale” della corrispondenza viene desunto dopo averne preso visione, il plico viene richiuso e inviato al destinatario privo di registrazione. L'eventuale registrazione di protocollo potrà essere effettuata in un momento successivo.

39.4 Corrispondenza cartacea non di competenza dell'Amministrazione

La corrispondenza cartacea che non è evidentemente di competenza del Comune (es. altro destinatario) non va aperta e va riconsegnata al servizio postale; in caso di errata apertura, la busta va richiusa indicando la dicitura “aperta per errore”, apponendo timbro datario, e riconsegnata al servizio postale. La corrispondenza cartacea che invece riporta l'indirizzo corretto sulla busta, ma non è di competenza del Comune, a seguito dell'apertura e valutazione, va richiusa indicando la dicitura “aperta e non di competenza”, apponendo timbro datario e riconsegnata al servizio postale.

Sezione terza – Classificazione, fascicolazione e accesso ai documenti informatici

39. Classificazione dei documenti

I documenti formati e acquisiti dal Comune sono classificati mediante indicazione del titolo e della classe secondo i criteri previsti nel Titolario di cui **all'Allegato 11**. I documenti devono essere classificati contemporaneamente alla registrazione di protocollo. Non è ammessa la registrazione di protocollo di documenti non classificati.

La classificazione dei documenti in entrata è effettuata dal personale addetto alla protocollazione, mentre la classificazione dei documenti prodotti dal Comune è effettuata dal personale delegato all'interno dei singoli uffici.

Sono classificati anche i documenti soggetti a registrazione particolare.

Il Responsabile della gestione documentale verifica periodicamente la rispondenza ai procedimenti amministrativi e agli affari e valuta eventuali necessità di aggiornamento del Piano di classificazione.

Il Responsabile della gestione documentale stabilisce e propone, laddove necessario, l'implementazione di nuovi sottolivelli di Titolario.

40. Fascicolazione informatica dei documenti

Le pubbliche amministrazioni creano fascicoli informatici contenenti atti, documenti e dati relativi ad un procedimento amministrativo, al fine di adempiere agli obblighi imposti dalla normativa per una corretta gestione documentale. Ai sensi del comma 2-bis dell'art. 41 del CAD, “*il fascicolo informatico è realizzato garantendo la possibilità di essere direttamente consultato ed alimentato da tutte le amministrazioni coinvolte nel procedimento [...].*” Il fascicolo informatico reca l'indicazione del Comune titolare del procedimento, delle altre amministrazioni, del Responsabile del procedimento, dell'oggetto e dell'elenco dei documenti oltre all'identificativo del fascicolo medesimo.

Alla stesura del presente Manuale, il Comune non fascicola né è dotato di un piano di fascicolazione.

41. Accesso ai documenti informatici

Compatibilmente con l'evoluzione dei sistemi informativi, l'accesso ai documenti informatici da parte di utenti esterni all'Amministrazione sarà realizzato mediante l'impiego di sistemi sicuri per quanto riguarda il riconoscimento e l'autenticazione.

Agli utenti riconosciuti ed abilitati alla consultazione saranno rese disponibili tutte le informazioni necessarie e sufficienti all'esercizio del diritto di accesso ai documenti amministrativi, in conformità alle disposizioni normative e regolamentari vigenti.

Sezione quarta – Flussi documentali interni

42. Assegnazione dei documenti in entrata agli uffici

L'assegnazione dei documenti in entrata, quando possibile, è effettuata con modalità automatizzate. In particolare, sono automaticamente assegnate agli uffici o utenti, preventivamente individuati, le fatture elettroniche provenienti dal Sistema di Interscambio (SDI).

Ulteriori criteri di assegnazione automatica sono definiti dal Responsabile del protocollo, qualora vi siano degli Uffici interessati. I documenti non assegnati automaticamente sono assegnati agli Uffici dal personale addetto alla protocollazione in base all'oggetto del documento e alla classificazione (vedi **Allegato 11**).

Quando un documento è di interesse anche per più Uffici, si provvede a più assegnazioni "per conoscenza". Lo scambio informale di documenti tra gli Uffici non richiede la protocollazione del messaggio. Scambi di documenti tra gli uffici possono essere effettuati anche attraverso posta elettronica e cartelle condivise. In ogni caso, nelle attività di trasmissione e scambio dei documenti, tutto il personale deve utilizzare esclusivamente gli strumenti messi a disposizione dal Comune.

43. Comunicazioni interne

I documenti interni sono tutti gli atti prodotti all'interno del Comune con tecnologie informatiche e possono essere:

- di natura prevalentemente informativa
- di natura prevalentemente giuridico-probatoria.

I documenti interni di preminente carattere informativo sono di norma documenti di lavoro di natura temporanea che possono non entrare a far parte del fascicolo definitivo relativo all'affare di cui trattano: memorie informali, appunti, bozze di documenti prive di annotazioni significative, brevi comunicazioni di rilevanza meramente informativa. Non sono soggetti a protocollo e la loro circolazione avviene tramite semplice consegna all'ufficio destinatario tramite posta elettronica.

I documenti interni di preminente carattere giuridico-probatorio sono invece quelli redatti dal personale nell'esercizio delle proprie funzioni e al fine di documentare fatti inerenti all'attività svolta e alla regolarità delle azioni amministrative o comunque qualsiasi altro documento dal quale possano nascere diritti, doveri o legittime aspettative di terzi. Essi sono soggetti alla registrazione di protocollo che, attestandone il momento della consegna da un servizio ad un altro o tra gli organi o tra organi e servizio, ne definisce contestualmente il trasferimento di responsabilità in relazione al procedimento o all'affare di cui fanno parte o che viene contestualmente attivato.

Le comunicazioni personali sono trasmesse a mezzo di posta elettronica ordinaria. Quando la comunicazione indirizzata a più destinatari, in ragione del contenuto e degli invii multipli, potrebbe comportare la divulgazione di dati personali, il mittente provvede a invii individuali. Non è consentito l'utilizzo di servizi di messaggistica istantanea (es. Whatsapp, ecc.) per lo scambio di documenti nell'ambito dell'attività lavorativa.

44. Pubblicazioni all'Albo pretorio online

Tutti gli atti prodotti dal Comune che, ai sensi della normativa vigente, sono soggetti a pubblicazione nell'Albo pretorio online del Comune, sono trasmessi per la pubblicazione in modo automatizzato solo dopo che il documento sia divenuto immodificabile (v. art. 14 del presente Manuale).

BOLLA

Parte quinta – Conservazione dei documenti

45. Sistema di conservazione dei documenti informatici

Il Comune, per la conservazione dei documenti informatici e degli altri oggetti digitali destinati alla conservazione, ha scelto un modello in outsourcing, esternalizzando il servizio di conservazione ai sensi dell'art. 44, comma 1-quater, del CAD.

Il servizio sopracitato del Comune è stato affidato al Conservatore Maggioli (d'ora in avanti anche solo "Conservatore").

Le attività affidate al Conservatore sono puntualmente indicate nel contratto per l'affidamento del servizio.

Per la descrizione delle attività del processo di conservazione non definite nel presente Manuale, così come consentito dal par. 4.6 delle Linee Guida Agid, è fatto rinvio all' **Allegato 14** – Piano di conservazione e al Manuale del servizio di conservazione digitale di Maggioli spa di cui **all'Allegato 13** al presente Manuale nonché agli ulteriori documenti tecnici in merito all'affidamento del servizio di conservazione.

46. Responsabile della conservazione

Come precisato all'art. 5 del presente Manuale, il Comune ha designato un unico soggetto che riveste i ruoli di Responsabile della gestione documentale e Responsabile della conservazione (v. **Allegato 3**).

È compito del Responsabile della conservazione assicurare il rispetto della normativa vigente da parte del Conservatore e degli obblighi contrattuali dallo stesso assunti, ivi compreso il rispetto delle misure di sicurezza dei dati trattati. A tal fine, il Responsabile agisce d'intesa con il Responsabile per la protezione dei dati (RPD/DPO) del Comune.

Il Responsabile della conservazione, ferma restando la propria responsabilità, può delegare in tutto o in parte una o più attività di propria competenza relative alla conservazione, affidandole a soggetti interni al Comune dotati di adeguate competenze. Gli atti di delega devono individuare le specifiche attività e funzioni delegate.

47. Oggetti della conservazione

Gli oggetti della conservazione sono:

- i documenti informatici formati e ricevuti dal Comune e i rispettivi metadati (conformi all'Allegato 5 alle Linee guida dell'AgID);
- il registro del protocollo informatico generale e giornaliero;
- gli altri registri e repertori tenuti dal Comune.

Gli oggetti della conservazione sono trattati dal sistema di conservazione del Conservatore in pacchetti informativi che si distinguono in:

- pacchetti di versamento;
- pacchetti di archiviazione;
- pacchetti di distribuzione.

48. Formati ammessi per la conservazione

I formati ammessi per la conservazione sono individuati nell'Allegato 2 alle Linee guida dell'AgID e corrispondono a quelli specificati **nell'Allegato 8** al presente Manuale.

Nei casi in cui sia necessario procedere al riversamento di documenti in altri formati, purché conformi a quelli indicati nell'Allegato 2 alle Linee guida, il Responsabile della conservazione, prima del versamento, valuta la corrispondenza fra il formato originale e quello di riversamento e ne garantisce la conservazione attraverso l'attestazione di conformità, rilasciata secondo le modalità indicate nella Parte Terza del presente Manuale.

49. Modalità, tempi di trasmissione e gestione dei pacchetti di versamento

Il sistema di gestione documentale versante (Sicraweb EVO) raccoglie e trasmette le unità documentali da versare all'archivio digitale di deposito, secondo quanto congiuntamente definito tra il Responsabile della gestione documentale e della conservazione del Comune e il Responsabile del servizio di conservazione esterno (Maggioli spa).

Il processo di versamento e conservazione è diviso in 3 fasi:

- trasferimento quotidiano delle unità documentarie da conservare;
- periodica chiusura dei pacchetti di versamento (PDV) da parte del sistema versante;
- presa in carico da parte del sistema di conservazione con contestuali produzioni del pacchetto di archiviazione (PDA) e del rapporto di versamento.

Il sistema di conservazione genera e sottoscrive per ogni PDV e per conto del Responsabile della conservazione del Comune il rapporto di versamento e l'indice di conservazione (UNI SinCRO V2) secondo le modalità descritte nel Manuale del servizio di conservazione esterno.

Il versamento dei documenti avviene secondo le seguenti tempistiche:

- versamento ogni 15 giorni, limitatamente a documenti e tracciati generati tramite SIOPE+;
- versamento automatizzato dei PDV a determinate scadenze;
- versamento quotidiano per il registro di protocollo giornaliero (entro le 24 ore successive al momento della produzione);
- versamento almeno settimanale per i documenti protocollati;
- versamento almeno quindicinale delle deliberazioni della Giunta, di consiglio, delle determinazioni dirigenziali e dei contratti.

La produzione dei PDA avviene in modalità automatica con le seguenti tempistiche:

- entro le 24 ore dal versamento per il registro di protocollo giornaliero;
- entro una settimana dal versamento per i documenti protocollati;
- entro quindici giorni dal versamento per le deliberazioni della Giunta, per le determinazioni dirigenziali e i contratti.

La produzione dei pacchetti di distribuzione (PDD) avviene in modalità automatica, ma su istanza degli utenti abilitati al portale web del servizio, come descritto nel Manuale utente per il Servizio di conservazione digitale di Maggioli spa (v. **Allegato 16**).

50. Memorizzazione dei dati e salvataggio della memoria informatica

La sicurezza delle informazioni (intesa come il patrimonio informativo gestito), è ottenuta realizzando una serie idonea di controlli che comprendono politiche, procedure, istruzioni e raccomandazioni, strutture organizzative, strumenti e meccanismi tecnologici di tipo fisico e logico.

I controlli rispondono ai requisiti di sicurezza che possono essere rilevati dall'analisi dei rischi oltre che da requisiti legislativi e regolamentari di riferimento.

Le attività relative al servizio di gestione del patrimonio informativo coinvolgono varie figure

dell'organizzazione del Comune, titolare dei dati, tra cui l'amministratore di sistema IN.VA. S.p.A., Maggioli spa, il Responsabile della gestione documentale e della conservazione e il DPO, che interagiscono tra loro al fine di garantire la gestione di tutte le esigenze del produttore dei documenti.

Con l'obiettivo di garantire la continuità operativa e di ridurre la probabilità che avvengano eventi negativi (es. data-breach, eventi catastrofici, etc.), nonché di permettere al Comune di prepararsi ad essi e di rispondere in modo adeguato ripristinando l'operatività nel più breve tempo possibile, vengono intraprese le azioni di prevenzione indicate nel Piano di Continuità Operativa e di *Disaster Recovery*.

51. Accesso al Sistema di conservazione

Gli utenti, espressamente autorizzati dal Responsabile della gestione documentale e della conservazione, possono accedere al Sistema di conservazione tramite credenziali personali rilasciate dal Conservatore e comunicate al singolo utente. L'accesso al sistema consente di consultare i documenti digitali versati nel sistema e le configurazioni specifiche adottate.

52. Selezione e scarto dei documenti digitali

Periodicamente, secondo quanto previsto nel Piano di conservazione (v. **Allegato 14**), viene effettuata la procedura di selezione della documentazione da proporre allo scarto ed attivato il procedimento amministrativo di scarto documentale, con l'invio dell'elenco con la proposta di scarto di atti d'archivio alla competente Soprintendenza Archivistica, ai sensi dell'art. 21, comma 1, lettera d, del Codice dei Beni Culturali (D. lgs. 82/2004).

Le modalità per effettuare le operazioni di selezione e scarto dei documenti informatici sono descritte **nell'Allegato 13**.

53. Conservazione, selezione e scarto dei documenti analogici

La documentazione analogica corrente è conservata a cura del Responsabile del procedimento fino al trasferimento in archivio di deposito.

I documenti analogici correnti dell'Amministrazione sono conservati negli uffici del Comune. Il Responsabile della conservazione, in collaborazione con gli uffici produttori, cura il versamento nell'archivio di deposito.

Le pratiche concluse del Comune sono conservate nei locali di proprietà del Comune destinati ad archivio di deposito.

I documenti non soggetti a operazioni di scarto sono conservati nell'archivio di deposito secondo i termini di legge, per poi essere trasferiti nell'archivio storico per la conservazione permanente. Occorre lasciare traccia documentale delle operazioni di trasferimento attraverso la compilazione di elenchi di versamento.

54. Misure di sicurezza e monitoraggio

Il Manuale del servizio di conservazione digitale descrive le modalità con cui il fornitore del servizio assicura gli obiettivi di sicurezza richiesti per la conservazione a lungo termine degli archivi, dettagliando i controlli di sicurezza delle diverse componenti del sistema (organizzazione, accessi, infrastruttura, gestione dell'esercizio, gestione dello sviluppo) e le procedure adottate per garantire i *backup* degli archivi e il *Disaster recovery*.

Il Conservatore provvede altresì al periodico monitoraggio al fine di verificare lo stato delle componenti infrastrutturali del sistema e l'integrità degli archivi.

Il Responsabile vigila affinché il Conservatore provveda alla conservazione integrata dei documenti e dei metadati associati nelle fasi di gestione e di conservazione. A tal fine, con cadenza almeno annuale, richiede al Conservatore l'esibizione di un campione di documenti.

Nel caso siano riscontrate irregolarità, provvede a sollecitare il Conservatore affinché vi ponga rimedio, anche attraverso gli strumenti contrattuali previsti negli atti di affidamento del servizio.

BOLLA

Parte sesta – Sicurezza e protezione dei dati personali

55. Disposizioni generali

Nel sistema di gestione informatica dei documenti sono previste idonee misure tecniche e organizzative per garantire livelli di sicurezza e di rischio adeguati, in ottemperanza ai principi definiti dalla normativa in materia di tutela e protezione dei dati personali.

Resta inteso che i dipendenti, in quanto funzionari pubblici, sono tenuti a rispettare il segreto d'ufficio e quindi a non divulgare notizie di natura riservata, a non trarre profitto personale o a procurare danno a terzi e all'amministrazione di appartenenza dalla conoscenza di fatti e documenti riservati.

56. Sicurezza dei dati e documenti informatici

Le risorse strumentali e le procedure utilizzate per la formazione e la gestione dei documenti informatici garantiscono:

- l'identificabilità del soggetto che ha formato il documento e il Comune di riferimento;
- la sottoscrizione dei documenti informatici, quando prevista;
- l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il sistema di protocollo informatico;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo;
- l'interscambiabilità dei documenti all'interno della stessa AOO e con AOO diverse.

Le funzionalità del protocollo informatico e dell'ambiente elaborativo adottato garantiscono il rispetto dei requisiti di riservatezza, di integrità, di disponibilità e non ripudio, oltre a quelli sopra richiamati.

I documenti informatici e i formati utilizzati per la produzione dei documenti possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura.

A tale fine i documenti informatici non devono contenere macroistruzioni o codici eseguibili, tali da attivare funzionalità che possano modificarne la struttura o il contenuto.

Il sistema garantisce:

- l'immodificabilità delle registrazioni di protocollo e la contemporaneità delle stesse con l'operazione di segnature;
- l'annullamento e non cancellazione fisica delle registrazioni di protocollo;
- la protezione delle informazioni relative a ciascun utente nei confronti degli altri.

Per attribuire una data certa ai documenti informatici prodotti all'interno del Comune si applicano le regole per la validazione temporale e per la protezione dei documenti informatici, secondo la normativa vigente e secondo quanto indicato nel Piano per la sicurezza del sistema di gestione informatica dei documenti di cui all'Allegato 4.

57. Protezione dei dati personali: adempimenti in materia

Nei casi in cui il trattamento viene sviluppato, per conto del Titolare, da un responsabile individuato ai sensi dell'art. 28 del Regolamento UE 679/2016, l'adozione delle misure tecniche ed organizzative è in capo anche a quest'ultimo.

I soggetti esterni a cui è delegata la tenuta del sistema di gestione informatica dei documenti sono individuati come Responsabili di trattamento ai sensi dell'art. 28 Regolamento UE 679/2016.

58. Misure organizzative di sicurezza per la protezione e la tutela dei dati nel sistema di gestione informatica dei documenti

Il sistema di gestione informatica del protocollo e dei documenti utilizzato dal Comune è conforme alle specifiche previste dalla normativa per quanto riguarda la sicurezza e il controllo accessi.

Il sistema di gestione documentale permette l'assegnazione differenziata dei profili di abilitazione, intervento, modifica e visualizzazione dei documenti in rapporto alle funzioni e al ruolo svolto dagli Uffici/utenti, garantendo la tutela dei dati personali.

Le abilitazioni dei singoli utenti sono estraibili dal sistema di gestione documentale in qualsiasi momento. Le modalità di rilascio delle abilitazioni di accesso degli utenti al sistema di gestione informatica dei documenti, e la relativa profilazione, avvengono secondo i criteri individuati dalla AOO nella Procedura per la gestione delle abilitazioni di accesso al protocollo informatico in allegato al presente manuale (v. **Allegato 17**)

Il sistema di gestione informatica del protocollo e dei documenti assicura:

- l'univoca identificazione e autenticazione degli utenti che accedono al sistema di gestione informatica dei documenti tramite user ID e password. Gli utenti, così abilitati, accedono al sistema mediante le credenziali di accesso ricevute. Al primo accesso viene richiesto il cambio password secondo i criteri di complessità richiesti da sistema. In nessun caso la password deve essere ceduta a terzi e dovrà essere modificata dal proprietario ogni 90 giorni.
- sulla base della struttura organizzativa e funzionale e su indicazione del Responsabile di servizio di appartenenza dell'utente, il Responsabile della gestione documentale attribuisce almeno i seguenti livelli di autorizzazione:
 1. abilitazione alla consultazione;
 2. abilitazione all'inserimento;
 3. abilitazione alla modifica delle informazioni per quanto concerne i campi modificabili;
 4. abilitazione all'annullamento dell'intera scheda di protocollo;
- la garanzia di accesso alle risorse esclusivamente agli utenti abilitati e/o a gruppi di utenti secondo la definizione di appositi profili.

Per ogni documento, all'atto della registrazione, il sistema consente di stabilire quali utenti o gruppi di utenti hanno accesso ad esso, nel rispetto della normativa in materia di trattamento e tutela dei dati personali. Di norma ogni dipendente può consultare i documenti relativi ad affari di propria competenza, del proprio Ufficio o allo stesso assegnati e quei documenti di carattere generale e infrastrutturale necessari a concludere il procedimento. Il controllo degli accessi al sistema di gestione informatica dei documenti è assicurato mediante le modalità descritte nel Piano per la sicurezza del sistema di gestione informatica dei documenti allegato al presente Manuale.

L'accesso ai documenti registrati nel sistema avviene secondo i seguenti criteri:

- la visibilità dei documenti è garantita ai gruppi di utenti/utenti identificati nel sistema sulla base delle articolazioni interne come previste dall'organigramma;
- ogni Ufficio stabilisce internamente le modalità di accesso e gestione della documentazione di propria competenza optando per lo smistamento centralizzato delle pratiche per competenza a soggetti diversi (da parte del Responsabile di servizio se

presente) ovvero presa in carico diretta della pratica da parte dell'utente competente all'evasione della stessa;

- creazione di Access Control List (ACL) per consentire l'accesso ai documenti a gruppi di utenti creati *ad hoc*.

59. Registrazione attività rilevanti sul sistema di gestione documentale

Ai fini della sicurezza sono registrate le attività svolte sul sistema da parte di ciascun utente. Il sistema assicura il tracciamento di qualsiasi evento, compresa la modifica delle informazioni trattate, nonché l'identificazione dell'autore.

Le informazioni memorizzate dal sistema sono le seguenti:

- univoca identificazione e autenticazione degli utenti;
- registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantirne l'identificazione;
- controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppo di utenti;
- tracciamento permanente di qualsiasi evento di modifica delle informazioni trattate e individuazione del suo autore;
- annullamento delle informazioni registrate in forma immodificabile, l'operatore che lo ha effettuato e gli estremi del provvedimento di autorizzazione;
- lettura anche a distanza di tempo delle informazioni annullate;
- varie attività gestionali sul documento (smistamento, presa in carico, rifiuto, completamento) con memorizzazione di data/ora e autore.

I dati e i documenti informatici sono memorizzati nel sistema di gestione informatica dei documenti al termine delle operazioni di registrazione.

60. Amministratore di sistema

Il ruolo di Amministratore del Sistema è affidato alla società in house IN.VA. S.p.a., nominata mediante deliberazione di Giunta n. 9 del 27/02/2025 in particolare all'art. 17 "Amministratori di sistema" della Convenzione che sancisce l'accordo tra il Comune e la società IN.VA. S.p.a., per la gestione del sistema informativo del Comune.

61. Uso del profilo utente per l'accesso dei dipendenti ai sistemi informatici

Per l'accesso ai sistemi informatici del Comune è necessaria l'assegnazione di un profilo utente, da parte dell'amministratore di sistema. Ogni profilo è protetto da un sistema di credenziali (username e password). Al momento della creazione del profilo utente sono attribuiti lo username e una password temporanea. Al primo accesso dell'utente, viene richiesto l'inserimento di una nuova password, mentre lo username resta invariato.

L'uso di ogni profilo utente è strettamente personale e ogni dipendente, sotto la propria responsabilità, è tenuto a custodire e non diffondere le proprie credenziali. Ciascun dipendente deve associare al proprio profilo una password di almeno otto caratteri, che preveda almeno una lettera maiuscola, una lettera minuscola, un numero e un carattere speciale (ad esempio: #, !, ?, -, &, ecc.).

Le policy dell'Amministratore di sistema prevedono che, con una cadenza trimestrale, per ogni profilo utente, sia richiesto il rinnovo della password.

Per quanto concerne il trattamento dei dati personali si rimanda al Regolamento per il trattamento dei dati personali.

62. Accessibilità da parte degli utenti non appartenenti al Comune di Saint-Vincent

L'accesso agli atti nel Comune è garantito secondo la normativa vigente in materia e i regolamenti in vigore presso il Comune, pubblicati sul sito istituzionale del Comune all'interno della sezione "Amministrazione Trasparente".

Il Comune ha regolamentato tale disciplina attraverso il Regolamento in materia di accesso ad atti e documenti approvato con Deliberazione Consiglio Comunale n. 8 del 19 gennaio 2009

63. Accesso agli archivi analogici del Comune di Saint-Vincent

L'archivio di deposito del Comune (documentazione degli ultimi 30 anni) è collocato nei locali di proprietà del Comune, situati al piano -3 del Comune, che offrono garanzie di adeguata conservazione dei documenti cartacei. L'accesso alla documentazione dell'archivio storico del Comune, collocato nei locali situati al 5° piano del Comune, è consentito all'utenza esterna attraverso la richiesta di appuntamento all'ufficio preposto. Maggiori informazioni sono reperibili sul sito istituzionale del Comune al seguente link: <https://www.comune.saint-vincent.ao.it/aree-tematiche/cultura/archivio-storico>