



Comune di Vische (TO)

MANUALE DI GESTIONE DOCUMENTALE

Allegato 08 – Piano per la Sicurezza Informatica

PIANO PER LA SICUREZZA INFORMATICA

1. Premessa e ambito di applicazione

Il presente Piano per la Sicurezza Informatica è adottato ai sensi delle seguenti fonti normative: Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici (Determinazione n. 407/2020, aggiornate con Determinazione n. 371/2021), par. 3.5; art. 51 del D. Lgs. 82/2005 (CAD); Regolamento (UE) 2016/679 (GDPR), art. 32; D. Lgs. 196/2003 come modificato dal D. Lgs. 101/2018; L. 3 agosto 2024, n. 90 (Cybersicurezza nazionale); D. Lgs. 138/2024 (NIS2); Misure minime di sicurezza ICT per le PA (Circolare AgID n. 2/2017, confluite nelle linee guida ACN). Esso descrive le politiche adottate dall'Ente affinché:

- I documenti e le informazioni trattati siano resi disponibili, integri e riservati.
- I dati personali comuni, sensibili e giudiziari vengano custoditi in modo da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o trattamento non consentito.

Il Piano definisce le misure tecniche, organizzative e procedurali per la tutela del patrimonio documentale gestito attraverso il Sistema di Gestione Informatica dei Documenti (SGID) adottato dall'Ente. Le misure si applicano anche alle attività di conservazione digitale descritte nell'Allegato 7.

2. Analisi dei rischi

I documenti informatici e i dati gestiti dal Sistema di Gestione Informatica dei Documenti (SGID) sono esposti a rischi che possono comprometterne la validità giuridica o la riservatezza. Le principali minacce identificate includono:

- **Accesso non autorizzato:** Intrusione nel sistema o visualizzazione indebita di fascicoli riservati.
- **Manomissione o Cancellazione:** Modifica non tracciata dei dati di protocollo o eliminazione accidentale di documenti.
- **Perdita dei dati:** Indisponibilità dovuta a guasti tecnici o eventi calamitosi.
- **Trattamento illecito:** Utilizzo dei dati per finalità non conformi ai compiti istituzionali.



Comune di Vische (TO)

MANUALE DI GESTIONE DOCUMENTALE

Allegato 08 – Piano per la Sicurezza Informatica

3. Infrastruttura tecnologica e sicurezza della rete

Il Sistema di Gestione Informatica dei Documenti (SGID) adottato dall'Ente è prodotto da Siscom Spa di Cervere (CN).

L'architettura è basata su un modello di tipo SaaS ("Software as a Service") erogato in modalità Public Cloud su infrastruttura proprietaria completamente localizzata in Italia, dedicata ad ospitare i servizi sviluppati per le PA, realizzata secondo gli standard esistenti al fine di garantire la massima sicurezza possibile per il mantenimento dei dati.

3.1 Qualificazione e sicurezza Cloud

- L'infrastruttura tecnologica è qualificata nel Marketplace dei servizi Cloud per la PA dell'Agenzia per la Cybersicurezza Nazionale (ACN) e risponde pienamente ai requisiti del "Cloud della PA".

Certificazioni obbligatorie

- certificazione ISO 9001:2015
- certificazione ISO 27001:2013
- certificazioni ISO 27017:2015 e 27018:2019
- certificazione ISO/IEC 20000 - Service Management

Standard tecnici utilizzati per la progettazione e gestione del servizio Cloud

Lo standard SiscCloud si basa sui principi dettati dalle norme/ISO/IEC e viene gestito in base ai principi dettati dalle seguenti norme:

- ISO/IEC 20000
- ISO 27001
- ISO 27017
- ISO 27018

Elenco certificazioni aggiuntive ottenute relative al servizio Cloud

- ISO/IEC 27001 estesa con i controlli degli standard ISO/IEC 27017 e ISO/IEC 27018, e certificazione ISO 20000 sui servizi IT cloud.



Comune di Vische (TO)

MANUALE DI GESTIONE DOCUMENTALE

Allegato 08 – Piano per la Sicurezza Informatica

Elenco certificazioni aggiuntive ottenute relative all'organizzazione

- ISO 9001 sul sistema di gestione della qualità SGQ
- ISO/IEC 27001 sulla sicurezza informatica
- ISO/IEC 27017 dei codici di condotta sulla sicurezza
- ISO/IEC 27018 sulla protezione delle informazioni
- ISO 20000 servizi IT cloud
- ISO 14001 sulla gestione sistema ambientale.

L'accesso al sistema da parte degli utenti avviene tramite protocollo sicuro (HTTPS) ed è riservato e garantito agli utenti autenticati, ereditando i meccanismi di protezione perimetrale dell'infrastruttura Cloud certificata.

4. Politiche di gestione degli accessi e delle credenziali

4.1 Identificazione e autenticazione

L'accesso al sistema Siscom Spa è consentito esclusivamente previa procedura di identificazione informatica. A ogni incaricato sono assegnate credenziali personali costituite da:

- User-ID: Codice identificativo univoco.
- Password: Parola chiave riservata, nota solo all'utente.

Al sistema SISCOM è possibile accedere anche con sistemi di identificazione digitale come SPID e CIE.

4.2 Profilazione degli utenti interni

L'accesso ai documenti è regolato dal principio di necessità (*need to know*). Il sistema gestisce l'assegnazione dei diritti tramite profili di autorizzazione predefiniti.

- Ogni utente visualizza e gestisce solo i documenti assegnati alla propria UOR o ai propri procedimenti di competenza.
- La visibilità su fascicoli di altri uffici è inibita di default e può essere concessa solo esplicitamente dal Responsabile del procedimento o dell'UOR competente.



Comune di Vische (TO)

MANUALE DI GESTIONE DOCUMENTALE

Allegato 08 – Piano per la Sicurezza Informatica

- Le funzioni di amministrazione del sistema (creazione utenti, modifica log, configurazione) sono riservate esclusivamente agli Amministratori di Sistema e al Responsabile della Gestione Documentale.

4.3 Password policy

In conformità alle best practice di sicurezza, la password deve rispettare i seguenti requisiti di complessità:

- Lunghezza minima di 8 caratteri (preferibilmente una passphrase di almeno 4 parole casuali).
- Composizione mista contenente almeno una lettera maiuscola, una minuscola, un numero e un carattere speciale (simbolo non alfanumerico).
- Assenza di riferimenti agevolmente riconducibili all'utente (es. nome, data di nascita).

4.4 Ciclo di vita delle credenziali

- Modifica obbligatoria:** La password deve essere cambiata al primo utilizzo e, successivamente, solo in caso di compromissione accertata o sospetta, o di variazione del ruolo dell'utente. Il cambio periodico obbligatorio in assenza di segnali di compromissione è sconsigliato dalle più aggiornate linee guida internazionali (NIST SP 800-63B:2024 e ACN), in quanto induce comportamenti scorretti. L'adozione dell'autenticazione a più fattori (MFA) è la misura più efficace in sostituzione del cambio periodico e deve essere adottata ove tecnicamente disponibile.
- Disattivazione:** Le credenziali non utilizzate per un periodo superiore a sei mesi vengono disattivate automaticamente dal sistema. I profili disattivati non possono essere riattivati; in caso di rientro in servizio, sarà necessaria una nuova assegnazione.
- Smarrimento:** In caso di dimenticanza, si procede al reset e all'assegnazione di una nuova chiave di accesso; la vecchia password non è recuperabile.

4.5 Procedura di emergenza

Per garantire la continuità amministrativa nel trattamento di dati sensibili o giudiziari, le credenziali degli operatori abilitati a tali trattamenti devono essere consegnate in busta chiusa e sigillata al Responsabile della UOR. L'apertura della busta è consentita al



Comune di Vische (TO)

MANUALE DI GESTIONE DOCUMENTALE

Allegato 08 – Piano per la Sicurezza Informatica

Responsabile solo in casi di necessità indifferibile (es. assenza prolungata e imprevista dell'operatore) per garantire l'operatività dell'ufficio. Al rientro, l'operatore dovrà generare una nuova password e consegnare una nuova busta sigillata.

4.6 Accesso di utenti esterni

L'accesso da parte di soggetti esterni all'Amministrazione (cittadini, imprese, altre PA) è consentito secondo modalità differenziate:

- **Accesso autenticato:** richiesto per la presentazione e/o consultazione di istanze e pratiche tramite la piattaforma OpenCity Italia, ove prevista per lo specifico servizio. L'utente esterno può autenticarsi tramite sistemi di identità digitale (SPID/CIE) o secondo le ulteriori modalità rese disponibili dalla piattaforma.
- **Consultazione pubblica:** Per i dati soggetti a pubblicità legale (Albo Pretorio) o trasparenza, l'accesso avviene tramite il sito web istituzionale in formato aperto, garantendo comunque il rispetto della normativa sulla protezione dei dati personali (oscuramento dati sensibili ove previsto).

5. Sicurezza fisica e logica delle postazioni di lavoro

Le postazioni di lavoro sono strumenti istituzionali, pertanto agli operatori è fatto obbligo di:

1. **Custodia:** non lasciare mai la postazione incustodita con la sessione aperta. È obbligatorio bloccare o spegnere il PC in caso di allontanamento temporaneo o al termine del servizio.
2. **Protezione visiva:** adottare accorgimenti (es. posizionamento monitor) per evitare che dati personali siano visibili a terzi non autorizzati, specialmente in uffici aperti al pubblico (postazioni di sportello).
3. **Divieti:** non installare software non autorizzato e non copiare dati di titolarità dell'Ente su dispositivi personali esterni (chiavette USB, hard disk personali).
4. **Dispositivi rimovibili:** l'eventuale uso di dispositivi rimovibili per finalità istituzionali è consentito solo con dispositivi approvati dall'Ente e dotati di cifratura; il loro utilizzo deve essere documentato. È vietato l'uso di dispositivi personali non approvati.
5. **Segnalazione:** Comunicare immediatamente ai referenti tecnici qualsiasi anomalia o sospetta violazione della sicurezza.



Comune di Vische (TO)

MANUALE DI GESTIONE DOCUMENTALE

Allegato 08 – Piano per la Sicurezza Informatica

6. Sicurezza nella formazione e gestione del documento

6.1 Formati e firma digitale

I documenti informatici sono prodotti nei formati standard previsti dalle Linee Guida AgID (es. PDF/A) atti a garantire l'immutabilità e la leggibilità nel tempo. La sottoscrizione con firma digitale avviene prima della registrazione di protocollo per garantire paternità e integrità del documento.

6.2 Integrità del Protocollo

Lo SGID garantisce l'immodificabilità delle registrazioni chiave (numero, data, oggetto, mittente/destinatario).

- **Logging:** Ogni operazione, inclusa l'eventuale modifica autorizzata di campi secondari, è tracciata in file di log che registrano autore, data, ora e tipo di operazione, mantenendo recuperabile la versione precedente.
- **Annullamento:** L'annullamento di una registrazione è consentito solo previa autorizzazione formale e il sistema ne conserva traccia indelebile.
- **Registro Giornaliero:** Al termine di ogni giornata, il sistema genera automaticamente il Registro Giornaliero di Protocollo in formato statico, che viene inviato in conservazione entro il giorno successivo.

7. Backup e continuità operativa (Disaster Recovery)

I dati trattati dallo SGID sono conservati presso i data center italiani di Siscom Spa, su infrastruttura proprietaria certificata ISO/IEC 27001, 27017 e 27018.

Il sistema adotta una politica di backup multilivello articolata su cicli quotidiani, settimanali, mensili e annuali, affiancata da un servizio di Disaster Recovery remoto che assicura il ripristino dei dati in caso di eventi critici o interruzioni del servizio.

I parametri di Recovery Time Objective (RTO) e Recovery Point Objective (RPO) sono definiti nel contratto di servizio con il fornitore e nel Manuale del Conservatore (Allegato 7bis).

La riservatezza e l'integrità delle informazioni sono garantite mediante crittografia dei dati e ridondanza infrastrutturale, in conformità alle normative vigenti in materia di protezione dei dati personali.



Comune di Vische (TO)

MANUALE DI GESTIONE DOCUMENTALE

Allegato 08 – Piano per la Sicurezza Informatica

8. Conservazione a lungo termine

I documenti informatici definitivi sono versati nel sistema di conservazione digitale a norma, gestito dal soggetto conservatore esterno individuato dall'Ente e richiamato nel Manuale di conservazione. Il versamento avviene tramite pacchetti di versamento (SIP) standardizzati, garantendo la preservazione del valore legale dei documenti per il tempo previsto dal Piano di conservazione e massimario di scarto (Allegato 6), secondo le modalità previste dal Manuale di conservazione dell'Ente e dal Manuale del Conservatore (Allegati 7 e 7bis).

9. Tutela dei dati e gestione delle violazioni (Data Breach)

9.1 Misure per dati sensibili e giudiziari

Il trattamento di categorie particolari di dati (art. 9 e 10 GDPR) richiede misure rafforzate. Ove tecnicamente possibile, il sistema applica tecniche di cifratura o pseudonimizzazione (uso di codici identificativi) per separare i dati identificativi dalle informazioni sensibili. Anche per gli archivi cartacei e ibridi, l'accesso ai fascicoli riservati è consentito solo previa autorizzazione e registrazione dell'accesso.

Il Comune di Vische, in qualità di titolare del trattamento, mantiene il Registro delle attività di trattamento ai sensi dell'art. 30 del GDPR. I trattamenti svolti tramite il SGID sono ivi documentati con indicazione delle finalità, delle categorie di dati, dei destinatari, dei tempi di conservazione e delle misure di sicurezza adottate. Il Registro è tenuto aggiornato dal RPD/DPO e messo a disposizione del Garante su richiesta.

Per i trattamenti svolti tramite il SGID che possano comportare un rischio elevato per i diritti e le libertà degli interessati — in particolare quelli relativi a categorie particolari di dati (stato di salute, vita sessuale, dati genetici, dati giudiziari) — il RPD/DPO valuta la necessità di effettuare una Valutazione d'Impatto sulla Protezione dei Dati (DPIA), ai sensi dell'art. 35 del GDPR. La DPIA, ove effettuata, è documentata e conservata nel sistema documentale dell'Ente.



Comune di Vische (TO)

MANUALE DI GESTIONE DOCUMENTALE

Allegato 08 – Piano per la Sicurezza Informatica

9.2 Trasmissione sicura dei documenti

La trasmissione interna di documenti avviene esclusivamente tramite il flusso di lavoro (workflow) del SGID per evitare duplicazioni e dispersioni via e-mail. La trasmissione esterna verso altre PA o privati avviene tramite canali sicuri e certificati (PEC, interoperabilità SPC) utilizzando le signature XML conformi agli standard nazionali. È vietato utilizzare canali non istituzionali (es. e-mail personali, servizi di file transfer non approvati) per la trasmissione di documenti dell'Ente.

9.3 Gestione degli incidenti di sicurezza informatica

Un incidente di sicurezza informatica è qualsiasi evento che comprometta la disponibilità, l'integrità o la riservatezza del sistema o dei dati, indipendentemente dal fatto che comporti una violazione di dati personali. In caso di incidente informatico (attacco ransomware, accesso non autorizzato, DDoS, malfunzionamento critico), si applica la seguente procedura:

- **Rilevazione e contenimento:** l'operatore che rileva l'anomalia informa immediatamente il Responsabile della Gestione Documentale e il referente tecnico del fornitore del SGID.
- **Valutazione:** il Responsabile della Gestione Documentale, d'intesa con il Responsabile per la Transizione al Digitale e il RPD/DPO, valuta la natura e la portata dell'incidente entro 4 ore dalla segnalazione.
- **Notifica all'ACN:** ai sensi della L. 3 agosto 2024, n. 90, gli incidenti di sicurezza significativi sono notificati all'Agenzia per la Cybersicurezza Nazionale (ACN) tramite la piattaforma IRIS, nei termini e con le modalità stabilite dalla stessa ACN.
- **Documentazione:** l'incidente e le azioni intraprese sono documentati e conservati nel sistema documentale dell'Ente.

9.4 Sicurezza della supply chain

La sicurezza del sistema documentale dipende anche dalla sicurezza dei fornitori terzi (fornitore del SGID, soggetto conservatore, fornitori di assistenza informatica). A tal fine:

- I contratti con i fornitori di servizi ICT rilevanti includono clausole specifiche in materia di sicurezza delle informazioni, conformità normativa e audit.



Comune di Vische (TO)

MANUALE DI GESTIONE DOCUMENTALE

Allegato 08 – Piano per la Sicurezza Informatica

- Il Responsabile per la Transizione al Digitale verifica periodicamente il mantenimento delle certificazioni di sicurezza dei fornitori (ISO/IEC 27001:2022, qualificazione ACN).
- In caso di cessazione del rapporto con un fornitore, sono garantite la portabilità dei dati e la cancellazione sicura delle informazioni dai sistemi del fornitore cessante.

9.5 Notifica delle violazioni

In caso di violazione di sicurezza che comporti la perdita, la distruzione o la divulgazione non autorizzata di dati personali (Data Breach), il Titolare del trattamento, con il supporto del RPD/DPO, notifica l'accaduto al Garante per la Protezione dei Dati Personali entro 72 ore dalla scoperta, ai sensi dell'art. 33 del GDPR. Se la violazione comporta rischi elevati per i diritti degli interessati, l'Ente provvederà a comunicare l'accaduto anche a questi ultimi (art. 34 GDPR).

10. Formazione, monitoraggio e revisione

10.1 Formazione del personale

L'Ente predispone piani di formazione periodici per tutto il personale autorizzato. La formazione copre l'utilizzo tecnico del SGID, le procedure di sicurezza, la normativa sulla privacy e la gestione documentale.

10.2 Monitoraggio e Audit

Il Responsabile della Gestione Documentale effettua controlli periodici, anche a campione, per verificare:

- La corretta tenuta dei registri e dei log di sistema;
- La coerenza dei profili di autorizzazione assegnati;
- Il rispetto delle procedure di sicurezza da parte degli utenti. I file di log del sistema sono conservati in modalità sicura e possono essere messi a disposizione dell'Autorità Giudiziaria in caso di indagini.



Comune di Vische (TO)

MANUALE DI GESTIONE DOCUMENTALE

Allegato 08 – Piano per la Sicurezza Informatica

10.3 Revisione del piano

Il presente Piano di Sicurezza è soggetto a revisione con cadenza almeno biennale, o anticipata in caso di significative modifiche normative, organizzative o tecnologiche.