Allegato n. 4 –
Piano di sicurezza dei documenti informatici

Obiettivi del piano di sicurezza

Il piano di sicurezza garantisce che:

- i documenti e le informazioni trattate dall'AOO siano disponibili, integre e riservate;
- i dati personali comuni, sensibili e/o giudiziari, vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

Generalità

Il piano di sicurezza:

- si articola sulla competenza dell'AOO;
- si basa sui risultati dell'analisi dei rischi a cui sono esposti i dati e i documenti trattati, nei locali dell'AOO;
- si fonda sulle direttive strategiche di sicurezza stabilite dal Responsabile nei confronti dell'AOO;
- definisce:
  - le politiche generali e particolari di sicurezza da adottare all'interno dell'AOO;
  - gli aspetti operativi della sicurezza, con particolare riferimento alle misure minime di sicurezza, del Codice in materia di protezione dei dati personali;
  - i piani specifici di formazione degli addetti;
  - le modalità esecutive del monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

Il piano in argomento è soggetto a revisione formale con cadenza almeno annuale da parte del Responsabile della sicurezza.

Tipologie dei documenti trattati

Il sistema di gestione informatica dei documenti:

- garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;
- assicura la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;

- fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;
- consente il reperimento delle informazioni riguardanti i documenti registrati;
- permette, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di "privacy" con particolare riferimento al trattamento dei dati sensibili e giudiziari;
- garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

Le due tipologie di documenti gestite sono:
- documento informatico
- documento analogico

Per documento informatico s'intende *"la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti"*.
Per documento analogico s'intende "*il documento formato usando una grandezza fisica che assume valori continui, come le tracce su carta (documenti cartacei)*".
Entrambe le tipologie sono suddivise in documenti in arrivo, documenti in partenza e documenti interni.

Documenti in arrivo
Per documenti in arrivo s'intendono tutti i documenti acquisiti dal Comune di Varenna nell'esercizio delle proprie funzioni.

Documenti in partenza
Per documenti in partenza s'intendono tutti i documenti prodotti dal Comune di Varenna nell'esercizio delle proprie funzioni.

Documenti interni
Per documenti interni s'intendono tutti i documenti scambiati tra i Servizi del Comune di Varenna, tra uffici appartenenti ad un medesimo Servizio, tra Amministrazione Comunale e servizi.

I documenti interni si distinguono in documenti di carattere:
- informativo
- giuridico - probatorio

I documenti interni di carattere informativo sono memorie informali, appunti, brevi comunicazioni di rilevanza meramente informativa scambiate tra gli uffici e di norma non vanno protocollati.
I documenti interni di preminente carattere giuridico - probatorio sono quelli redatti dal personale del Comune di Varenna al fine di documentare fatti inerenti all'attività svolta e alla regolarità delle azioni amministrative, o qualsiasi altro documento dal quale possono nascere diritti, doveri o legittime aspettative di terzi: come tali devono essere protocollati.

<u>Analisi dei rischi per tipologia</u>

Questo capitolo fa riferimento ai soli documenti informatici.

Sono stati individuati una serie di elementi di rischio riconducibili ai documenti informatici. Per ognuno di essi deve essere predisposta una misura minima di sicurezza.

Accesso da parte degli utenti appartenenti all'Amministrazione
Il sistema informatico è basato su un meccanismo che costringe ogni utente ad autenticarsi (cioè dimostrare la propria identità).
È obbligatorio l'uso di una password per l'accesso ad ogni personal computer: sia per l'accesso alla rete interna sia per l'accesso al sistema di gestione documentale (e in quest'ultimo caso ogni utente è dotato di uno specifico profilo di autorizzazione).
In tal modo la riservatezza delle registrazioni di protocollo e dei documenti informatici è garantita.

Le precedenti operazioni sono inoltre possibili ai soli soggetti autorizzati appartenenti al Settore Servizi Informatici e Telematici per le sole attività sistemistiche di amministrazione, aggiornamento e manutenzione delle componenti di sistema.

Agli utenti "generici" del Comune di Varenna non è invece consentito accedere al sistema informatico, se non a quanto pubblicato sui siti internet istituzionali dell'Ente.
E' intenzione dell'Amministrazione procedere alla realizzazione di una postazione di consultazione dell'albo online per garantire la fruizione del servizio anche da parte di soggetti non attrezzati.

Cancellazione non autorizzata/manomissione di dati
La presenza delle password garantisce che non ci siano manomissioni fortuite dei documenti informatici.

Perdita dei dati
Quotidianamente viene effettuato il backup dei dati dell'intero sistema di gestione documentale; inoltre è intenzione di questa Amministrazione effettuare a campione delle letture di controllo e restore.

Trasmissione e interscambio dei documenti informatici - aspetti di sicurezza
Il Comune di Varenna predilige l'utilizzo di tecnologie di trasmissione sicure che hanno il seguente livello di sicurezza:

Tipologia di trasmissione	**Caratteristiche**	**Livello di sicurezza**
Posta elettronica Certificata	• identità sicura e accertata del titolare della casella / mittente • transito del messaggio attraverso il protocollo S/STTP Mime che garantisce la piena riservatezza • sicurezza dell'accettazione e consegna del messaggio attraverso l'utilizzo delle ricevute • tracciamento delle attività nel file di Log a carico del gestore del servizio	Alto

Canali Web - Istanze online	• accesso ai servizi previa autenticazione sicura del mittente	Basso
Interoperabilità	• meccanismo di trasmissione attraverso la Posta elettronica certificata con funzionalità interoperabili	Alto
Posta elettronica ordinaria	• identità del titolare della casella non accertata da un ISP (Internet server provider) accreditato • transito del messaggio attraverso un protocollo SMTP che non garantisce la riservatezza della trasmissione	Basso

Criteri di utilizzo degli strumenti tecnologici

Il sistema informatico garantisce agli utenti interni del Comune di Varenna l'accesso ai servizi previsti, mediante l'adozione di un insieme di misure organizzative e tecnologiche che prevedono quanto segue:

- ogni utente è responsabile, civilmente e penalmente, del corretto uso delle risorse informatiche, dei servizi e dei programmi a cui ha accesso, nonché dei dati trattati ai fini istituzionali;
- ogni utente è responsabile, civilmente e penalmente, del contenuto delle comunicazioni effettuate e ricevute a fini istituzionali, anche per quanto attiene la riservatezza dei dati ivi contenuti, la cui diffusione impropria potrebbe configurare violazione del segreto d'ufficio e della normativa per la tutela dei dati personali;
- ogni utente deve tenere comportamenti corretti, tali da preservare il buon funzionamento degli strumenti e tali da ridurre i rischi per la sicurezza del sistema informatico. É vietato l'utilizzo di supporti per la memorizzazione dei dati (CD, DVD, memorie USB, etc.) non sicuri e/o provenienti dall'esterno, al fine di non diffondere eventuali virus;
- i dati archiviati informaticamente devono essere esclusivamente quelli attinenti alle proprie attività lavorative;
- la tutela dei dati archiviati su personal computer che gestiscono localmente documenti e/o dati è demandata all'utente finale, il quale dovrà effettuare con frequenza opportuna i salvataggi su supporti dedicati ed idonei, nonché la conservazione degli stessi in luoghi adatti;
- tutti i dati sensibili riprodotti devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato da terzi. Altrettanta cautela deve essere riposta in fase di stampa dei documenti contenenti dati sensibili: la stampa va effettuata su stampanti presidiate dall'addetto;
- l'account ai diversi sistemi informatici è costituito da un codice identificativo personale (username) e da una parola chiave (password);
- la password che viene associata a ciascun utente è personale, non cedibile e non divulgabile;
- le password consigliate devono avere le seguenti caratteristiche:
  - lunghezza minima di 8 caratteri
  - caratteri di tipo alfanumerico e deve contenere almeno un numero, una lettera minuscola e una lettera maiuscola e, se possibile, un simbolo
  - non deve essere riconducibile a:
    - nome o cognome proprio o di un collega o di un famigliare

- identificativi di ufficio, di area, di servizio o del Comune, in modo parziale o completo
- date di nascita, codici fiscali o altri elementi che ne facilitino l'individuazione

- validità massima di 90 giorni.

Sicurezza fisica dei luoghi

Si garantisce la sicurezza fisica dei documenti cartacei conservandoli in locali dotati di:

- sistema d'autenticazione del personale tramite badge
- porte provviste di chiusura tramite chiave
- armadi provvisti di chiusura tramite chiave
- casseforti (uffici strategici)
- elettroschedario (uffici demografici)
- sistemi di condizionamento per il raffreddamento delle apparecchiature
- estintori
- impianti elettrici dedicati con fornitura elettrica d'emergenza garantita parzialmente anche da gruppi di continuità

E' attivo un controllo dell'attuazione del piano di verifica periodica sull'efficacia dei sistemi di sorveglianza e degli estintori.

Privacy

L'amministrazione titolare dei dati contenuti nella documentazione amministrativa di propria pertinenza assolve integralmente il dettato del Codice Privacy con atti formali interni ed esterni.

Relativamente agli adempimenti interni specifici, gli addetti destinati ad accedere al sistema di gestione documentale sono stati incaricati dal titolare del trattamento o, se nominato, dal responsabile del trattamento.

Relativamente agli adempimenti esterni, l'amministrazione:

- si è organizzata per garantire che i documenti trasmessi ad altre pubbliche amministrazioni riportino le sole informazioni relative a stati, fatti e qualità personali previste da legge o da regolamento e strettamente necessarie per il perseguimento delle finalità per le quali vengono acquisite;
- l'accesso al sistema informatico da parte di utenti esterni potrà avvenire nei casi di particolari procedimenti amministrativi con credenziali di accesso rilasciate dall'Ente. L'amministrazione rilascia all'amministrazione procedente apposita autorizzazione in cui vengono indicati i limiti e le condizioni di accesso volti ad assicurare la riservatezza dei dati personali ai sensi della normativa vigente;
- è garantito a tutti i cittadini, mediante l'istituzione dell'Accesso Civico, l'accesso e la libera consultazione a tutti gli atti dell'Ente per i quali è prevista la pubblicazione. Sul sito web istituzionale è consultabile l'apposita sezione "Amministrazione Trasparente" a cui il cittadino ha libero accesso e nella quale sono disponibili informazioni integre e conformi all'originale.

Eventuali dati personali oggetto di trattamento sono:

- trattati in modo lecito e secondo correttezza;
- raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
- esatti e, se necessario, aggiornati;
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

In relazione alla protezione dei dati personali trattati all'interno dell'amministrazione, questa dichiara di aver adempiuto al dettato delle norme del Codice Privacy con particolare riferimento:

- al principio di necessità nel trattamento dei dati;
- al diritto di accesso ai dati personali da parte dell'interessato;
- alle modalità del trattamento e requisiti dei dati;
- all'informativa fornita agli interessati ed al consenso quando dovuto;
- alla nomina degli incaricati del trattamento per gruppo o individualmente;
- alle misure minime di sicurezza.

Qualunque trattamento di dati personali è consentito soltanto per lo svolgimento delle funzioni istituzionali; inoltre se i dati gestiti non sono sensibili o giudiziari il loro trattamento è consentito anche in mancanza di una norma di legge o di regolamento.

Formazione del personale

Per una corretta gestione dei documenti informatici è prevista un'attività formativa per il personale dell'ente relativa alla formazione, gestione, trasmissione, accesso e conservazione dei documenti.

L'attività formativa deve prevedere sessioni di:

- cultura generale sull'utilizzo del personal computer;
- cultura generale sull'utilizzo della rete;
- utilizzo di programmi di produttività individuale;
- utilizzo di programmi di posta elettronica;
- aggiornamento sui programmi di gestione documentali;
- tutela dei dati personali;
- adeguamento alle norme sulla protezione dei dati personali e alle relative direttive.

Periodicamente è cura del Responsabile rilevare necessità formative in accordo con i vari responsabili di settore, ed effettuare dei controlli a campione sulla congruità delle registrazioni, sulla corretta sequenza della catena documentale e sull'utilizzo di un unico registro informatico, verificando, attraverso controlli nei vari uffici, la classificazione e la fascicolazione archivistica nonché le modalità di gestione dei documenti informatici.