PIANO di SICUREZZA INFORMATICA

GDPR (Generale Data Protection Regulation)

Riferimento al R.UE 679/2016

Comune di Romano di Lombardia

(Provincia BG)

Anno 2021

02	22 Gen. 2021	Mod Cap 2,12,16	Responsabile Segreteria	Titolare del Trattamento
01	30 Giu. 2018	Prima emissione del GDPR	Responsabile Segreteria	Titolare del Trattamento
Rev.	Data	Causale	Preparato da	Titolare Trattamento dei Dati

Indice

1 PREMESSA

Il Comune di Romano di Lombardia, in qualità di soggetto pubblico, ha predisposto il presente Piano delle Sicurezza del Sistema Informativo (nel seguito denominato più semplicemente PSSI o GDPR) che definisce le policy di sicurezza inerente il sistema di gestione delle informazioni del Comune.
Il piano della sicurezza identifica:

- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- gli asset/strumenti utilizzati per il trattamento delle banche dati;
- Il Registro dei trattamenti;
- l'analisi dei rischi che incombono sui dati (Privacy Impact Assessment);
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- le attività di formazione relative agli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;

Allo scopo di adeguarsi al dettato normativo, l'Amministrazione comunale ha provveduto ad effettuare un censimento generale delle banche dati sia cartacee che informatizzate contenenti dati personali, distribuite in tutte le sedi del suddetto Ente.

2 CAMPO DI APPLICAZIONE

Il presente documento sulla Sicurezza del Sistema Informativo, si applica a tutti i dati trattati direttamente dal Titolare o, per incarico dello stesso, gestiti all'esterno presso terzi, sia con strumenti elettronici o comunque automatizzati che con altri strumenti e supporti, anche non elettronici.
Esso è l'atto conclusivo di una serie di verifiche sullo stato della "sicurezza informatica" nel Comune. La presente procedura si applica alle sedi sotto identificate:

Denominazione Sede	Indirizzo
Sede Municipale	Piazza G. Longhi 5
Polizia Locale	Via Giacomo Rubini, 24
Servizi Demografici	Piazza XXIV Maggio 1
Biblioteca	Piazza XXIV Maggio 1
Servizi alla Persona	Via Giacomo Rubini, 24

3 CONCETTI, ABBREVIAZIONI, DEFINIZIONI

SW: software

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la struttu-razione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Dati Personali: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

Dati Personali Particolari (dati sensibili): dati idonei a rivelare l'origine razziale etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione ai partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Dati Giudiziari: i dati personali idonei a rivelare provvedimenti di cui all'articolo 3 comma 1, lettere da a) ad o) e da r) ad u) del DPR 14 novembre 2002, n 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

Titolare: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati Membri

Responsabile: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

Incaricati: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile

Interessato: persona fisica, l'ente o l'associazione cui si riferiscono i dati personali.

archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

Rischio: con il termine di rischio si identifica l'esposizione alla possibilità di ottenere un guadagno o una perdita economica o finanziaria, di sopportare un danno fisico o un ritardo, come conseguenza dell'incertezza associata al perseguimento di un determinato corso d'azione

Consenso dell'interessato: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

Pseudonimizzazione: il trattamento di dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

"**comunicazione elettronica**", ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;

diffusione, il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

reti di comunicazione elettronica, i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

rete pubblica di comunicazioni, una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;

"dati relativi al traffico", qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;

"dati relativi all'ubicazione", ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;

"posta elettronica", messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

Vengono di seguito elencate ulteriori definizioni, utilizzate all'interno del presente documento, che possono risultare utili al fine di una maggiore comprensione dello stesso:

"amministratore di rete", soggetto cui è conferito il compito di sovrintendere alla gestione delle risorse fisiche e logiche di una o più reti locali (LAN) ;

"S.I.C.", sistema informatico comunale; l'insieme delle strutture fisiche e logiche (hardware e software) che consentono il trattamento dei dati attraverso apparecchiature informatiche;

"dominio", insieme di utenti e gruppi di utenti attraverso il quale l'Amministratore di rete può gestire diversi aspetti della rete locale tra i quali il più importante è la definizione delle politiche di accesso alle risorse del sistema (es. file, cartelle, stampanti ecc.) ;

"Active Directory", elenco delle risorse presenti in una rete locale che consente, attraverso opportuni strumenti di amministrazione, di gestire le stesse in modo centralizzato;

"utente, user", soggetto che mediante l'utilizzazione di credenziali d'accesso valide può accedere ai servizi di un sistema informatico conformemente ad un profilo per esso definito dall'Amministratore;

"username", nome identificativo di un utente che, unitamente ad una password, consente l'accesso ad un sistema informatico protetto;

"SID", Security identifier, insieme di numeri di lunghezza variabile il cui valore identifica, in modo univoco, in un sistema windows NT o superiore una risorsa. Tale risorsa può essere un computer un utente o gruppo di essi; se una risorsa viene rimossa e successivamente ricreata con le medesime impostazioni, il SID assegnatogli sarà comunque diverso da quello posseduto precedentemente.

"password", parola chiave che, unitamente ad uno username, consente l'accesso ad un sistema informatico protetto; normalmente viene definita**:**

- **forte** se non è riconducibile all'utente che l'ha generata (nome, cognome, data di nascita, nome della figlia ecc.) e se in caso di attacco di forza bruta è in grado di resistere alla decodifica per un tempo ragionevolmente lungo se paragonato all'attuale sviluppo tecnologico in ambito informatico.

- **debole** se non presenta alcuna delle caratteristiche sopra citate e non consente per questo un accettabile livello di sicurezza.

"attacco di forza bruta (brute force cracking)", viene così definito il tentativo, da parte di persone non autorizzate, di accedere alle risorse di un sistema informatico protetto generando in rapidissima successione credenziali di autenticazione nel tentativo di trovare una combinazione (in genere username e password) valida.

"NTFS", metodo di organizzazione dei dati su un supporto magnetico (file system) che consente di regolare l'accesso ai dati in esso contenuti in base a criteri (permission) definiti dall'Amministratore;

"permission", regola che consente di temperare l'accesso da parte di uno o più utenti o gruppi di essi ad una determinata risorsa (file, cartelle, stampanti ecc);

"policy", politiche di accesso alle risorse di un sistema gestite generalmente a livello centralizzato;

"gruppo di protezione", insieme di utenti utilizzato per gestire gli accessi alle risorse di un sistema informatico centralizzato;

"file sharing", servizio di condivisione file, consiste nella facoltà di un computer di mettere a disposizione di altri utenti del sistema informatico i file in esso contenuti secondo predeterminate policy**;**

"virus informatici", programma in grado di produrre effetti più o meno dannosi a carico di uno o più sistemi informatici interconnessi contro la volontà dei gestori del sistema stesso**;**

"attacco DoS", attacco portato a carico di uno o più computer o dispositivi di rete mirato a provocare il collasso del loro sistema di interconnessione rendendo in tal modo inutilizzabili i servizi dagli stessi erogati.

"TCP/IP", insieme di protocolli che consentono a computer con sistemi operativi anche diversi di dialogare tra loro**;**

"download", trasferimento di dati da un computer remoto ad un computer locale attraverso l'utilizzo di opportuni protocolli di rete;

"sniffing", attività svolta a mezzo di particolari strumenti software e/o hardware che consente di "leggere" i dati in transito in una rete di computer ed eventualmente carpirne informazioni normalmente non accessibili (credenziali d'accesso a sistemi remoti, e-mail, flussi di connessioni ad internet ecc.);

"inconsistenza (dei dati), situazione in cui dei dati, a seguito di un evento doloso o accidentale, non rappresentano più la realtà**;**

"antivirus", software in grado di individuare, bloccare o eliminare virus informatici o codice maligno ed eventualmente riparare i danni dagli stessi provocati;

"definizioni (o firme) dei virus", insieme di informazioni che consentono al software antivirus di riconoscere i virus informatici o eventualmente del codice maligno;

"backup", procedura di salvataggio di dati, può essere eseguita sia su supporti removibili che su computer diversi da quello di origine**;**

"restore", procedura di recupero di dati salvati precedentemente attraverso una procedura di backup**;**

"file di log", file di testo contenente informazioni relative ad un determinato processo normalmente generato dal processo stesso o dal sistema operativo**;**

"stand alone", modalità di esecuzione di un software che non implica la presenza di un server o di un'architettura client – server dedicato, viene anche impiegato per indicare un computer non connesso ad alcuna rete locale;

"postazione di lavoro", insieme di strumenti informatici e non normalmente utilizzati da un soggetto per lo svolgimento delle funzioni allo stesso assegnate all'interno della struttura dell'Ente**;**

4 NORMATIVA DI RIFERIMENTO

Le norme e standard di riferimento:

Le norme e standard di riferimento:

- **Regolamento UE n. 2016/679** del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
- **D. Lgs del 10 agosto 2018 n.** 101 Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo
- **Direttiva UE n. 2016/680** del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio;
- **D.Lgs. 30 giugno 2003, n, 196**, recante: "Codice in materia di protezione dei dati personali" e successive modificazioni;

ISO/IES 27001 Information Technology Security Techniques – Code of Practice for information security controls

ISPD-10003 Maggio 2018 Schema per la valutazione della conformità al regolamento europeo

5 ORGANIGRAMMA PRIVACY COMPITI E RESPONSABILITÀ

Le figure identificate dalle disposizioni vigenti in materia di trattamento dei dati sono:

Titolare:
ha potere decisionale in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
Il titolare nomina con contratto o atto giuridicamente valido, il responsabile del trattamento, insieme al quale pone in atto le misure tecniche ed organizzative congrue per garantire un livello di sicurezza adeguato al rischio.

Responsabile Sistemi Informativi:
ha il compito di garantire che il Piano di Sicurezza Informatico venga manutenuto ed aggiornato in funzione dei cambiamenti organizzativi dell'ente, dell'evoluzione degli strumenti usati per il trattamento dei dati
ha il compito di verificare che la policy venga applicata correttamente nell'ambito delle proprie competenze;
ha il compito di promuovere e proporre soluzioni che migliorano la sicurezza del sistema informativo del Comune.
ha il compito di indire periodicamente un incontro per valutare le attività e le proposte dei vari responsabili in materia di sicurezza.

Responsabile di Area:
Garantisce la qualità dei dati, le corrette modalità di raccolta, conservazione e trattamento degli stessi, anche da parte del personale della propria struttura, secondo quanto disposto dalla normativa in tema di trattamento dei dati, dai Provvedimenti del Garante e dal presente documento e vigila sul rispetto delle istruzioni impartite
ha il compito di attuare le politiche di sicurezza nell'ambito del settore di competenza.
ha il compito di suggerire e promuovere azioni che migliorino la sicurezza dei dati trattati dall'ente.
Deve segnalare al DPO l'avvio di nuovi servizi che prevedono il trattamento dei dati
Deve verificare che eventuali fornitori a cui sono affidati il trattamento di banche dati del Comune abbiano competenze e modelli di gestione conformi alle indicazioni del nuovo regolamento europeo.

Il DPO (Data Protection Officer)
Ha il compito di:

- rendere noti al Titolare o al Responsabile del Trattamento gli obblighi derivanti dal Regolamento europeo e conservare la documentazione relativa a tale attività di comunicazione o di consulenza;
- vigilare sulla corretta applicazione delle policy in materia di privacy,
- vagliare la corretta attuazione delle disposizioni contenute nel regolamento europeo, occupandosi, in particolare di verificare che i sistemi, sin dalla fase della loro progettazione rispettino la privacy (privacy by design) verificare la protezione di default di dati e sistemi (privacy by default), rilevare che venga garantita la sicurezza nei trattamenti dei dati;
- fornire agli interessati un riscontro circa i diritti previsti dal regolamento;

- garantire la conservazione dei documenti relativi ai trattamenti;
- verificare il tracciamento delle violazioni dei dati personali e la loro comunicazione agli interessati;
- verificare che titolare o responsabile effettuino la valutazione dell'impatto delle attività sulla privacy e controllare che venga richiesta l'autorizzazione all'autorità quando occorre;
- fungere da intermediario tra Titolare o Responsabile e autorità Garante in materia di trattamento dei dati;
- controllare che siano rispettati eventuali provvedimenti o richieste espresse dall' autorità Garante in materia di trattamento dei dati.
- formare il personale in materia di privacy e trattamento dei dati;

5.1 l'Organigramma Inerente il Trattamento dei Dati

Nell' "organizzazione - privacy" dell'ente le figure coinvolte sono:
1. il "Titolare del trattamento": è la "figura" di vertice cui competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza dei dati.

2. il Responsabile Area: è un soggetto designato dal Titolare che, per esperienza, capacità ed affidabilità, fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento di dati personali, ivi compreso il profilo relativo alla sicurezza. Nell'ambito del Comune di Romano di Lombardia il Responsabile Interno del trattamento è generalmente individuabile nelle figure apicali, salvo limitate eccezioni. Lo si definisce anche Responsabile "interno" per distinguerlo dal Responsabile "esterno". Relativamente ai trattamenti di dati personali trasversali a più strutture, per l'individuazione si applica il criterio del maggiore ambito decisionale attribuito o vi possono essere situazioni di co-responsabilità.

3. il "Responsabile esterno del trattamento" ai sensi dell'art 28 del GDPR: è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo, esterno all'Amministrazione, che, previa designazione formale del Responsabile "interno" del trattamento, assume (su delega di quest'ultimo) poteri decisionali su un determinato trattamento e deve attenersi, nelle operazioni svolte, alle istruzioni ricevute.

4. l'Amministratore di Sistema: è, in ambito informatico, la figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software utilizzati nei vari uffici, le reti locali e gli apparati di sicurezza, nella misura in cui tali attività di gestione e manutenzione consentano di intervenire sui dati personali.

5. l'incaricato del trattamento" (persona autorizzata al trattamento): è la persona fisica che, operando sotto l'autorità del Responsabile di Area, effettua le operazioni di trattamento dei dati, attenendosi alle istruzioni ricevute.

6. il DPO Data Protection Officer: è il soggetto che, coadiuva il Titolare ed il Responsabile del trattamento e gli incaricati nella corretta gestione ed applicazione dei principi definiti dal Regolamento Europeo in termini di data Protection.

7. l'Interessato: è la persona fisica cui si riferiscono i dati personali (sono escluse dal campo di applicazione della normativa privacy le persone giuridiche).

Il Responsabile di Area nomina per iscritto, quali Incaricati del trattamento eventuali collaboratori "esterni" dell'Amministrazione (purché persone fisiche), a prescindere dal rapporto contrattuale intrattenuto con la stessa (ad es. stagisti, tirocinanti, ecc.), non dotati di potere decisionale autonomo, se stabilmente presenti negli uffici dell'Amministrazione.

Sanzioni:
il presente documento pone quindi una serie di istruzioni, direttive e linee guida poste a salvaguardia dei dati dei soggetti di cui il Comune gestisce i dati, costituenti tutti e ciascuna di essi dati patrimonio dell'ente stesso. Pertanto, l'eventuale inosservanza o violazione di tali istruzioni, direttive e linee guida costituisce infrazione disciplinare, nonché grave inadempimento ai sensi e per gli effetti dell'art. 1453 del Codice Civile, suscettibile di produrre le conseguenze previste dalla legge, nonché dal contratto collettivo nazionale e individuale di lavoro.

Nell'ambito del Comune di Romano di Lombardia vengono identificate le seguenti figure:

Area/Servizio	Posizione Organizzativa Prevista	Ruolo Trattamento dei Dati
Sindaco	Rappresentante Legale	Titolare del trattamento dei dati è il Comune che è rappresentato legalmente dal Sindaco
Procedimenti in carico al segretario	Segretario Comunale	Responsabile Trattamento dei Dati per l'area di competenza
Settore Servizi Demografici	Responsabile di Ufficio	Responsabile Trattamento dei Dati per l'area di competenza
Settore Ragioneria Tributi Patrimonio	Responsabile di Ufficio	Responsabile Trattamento dei Dati per l'area di competenza
Settore Segreteria	Responsabile di Ufficio	Responsabile Trattamento dei Dati per l'area di competenza
Settore Pubblica Istruzione Cultura Tempo Libero Sport	Responsabile di Ufficio	Responsabile Trattamento dei Dati per l'area di competenza

Settore Servizi Sociali	Responsabile di Ufficio	Responsabile Trattamento dei Dati per l'area di competenza
Settore Ambiente Territorio Urbanistica	Responsabile di Ufficio	Responsabile Trattamento dei Dati per l'area di competenza
Settore Polizia Locale	Responsabile di Ufficio	Responsabile Trattamento dei Dati per l'area di competenza
Sistemi Informativi	Responsabile Sistema Informativo	Trattamento dati informatici

6 COMPOSIZIONE DEL DOCUMENTO

Il GDPR identifica le Risorse da Proteggere"; che, in diverso modo, operano o comunque svolgono un ruolo significativo nei processi di trattamento dei dati.

A tal proposito, una volta individuati i dati da proteggere e gli asset utilizzati nella gestione degli stessi, tramite un'altra fase, definita di **Analisi dei Rischi**, sono state valutate e studiate le minacce e le vulnerabilità a cui tali risorse (i dati per l'appunto) sono sottoposte, in modo da potere valutare gli elementi che possono insidiare la protezione, l'integrità e la conservazione di ogni singolo dato personale trattato.

Dall'analisi dei rischi si è redatto un Piano di Sicurezza, tramite il quale si è provveduto a definire l'insieme delle misure fisiche, logiche ed organizzative adottate per tutelare le strutture e le risorse preposte al trattamento dati e quindi ai dati stessi.

Inoltre è stato definito un Piano di Verifiche delle misure adottate tramite il quale si provvederà ad accertare periodicamente la bontà delle misure individuate e ad apportare gli accorgimenti che si riveleranno necessari.

Per completezza, si è ritenuto utile e opportuno allegare al Piano della Sicurezza Informatica una serie di documenti che rendono, con immediatezza, intelligibile a quanti sono coinvolti, a vario titolo, nella politica di protezione e sicurezza dei dati personali adottata dal Titolare, nonché agli organi ispettivi, la politica di protezione e sicurezza dei dati personali (security and data protection policy).

7 REVISIONE DEI DOCUMENTI

L'emissione e la revisione della Piano di Sicurezza del Sistema Informativo, avviene nel rispetto di regole precise e sotto la sorveglianza del Responsabile Settore Amministrativo che garantisce uno sviluppo equilibrato e congruente con l'evoluzione del sistema informativo del Comune.

Le regole da seguire per i vari tipi di documenti sono le seguenti:
Il GDPR contiene le politiche di sicurezza del Comune. Eventuali modifiche della policy e revisioni del documento possono essere suggerite per iscritto da qualsiasi collaboratore dell'ente al Responsabile del Servizio Informativo che le valuta e decide per un'eventuale modifica.

L'analisi dei rischi identifica i possibili eventi indesiderati che possono causare un danno alle risorse del sistema informativo. Una revisione del documento può essere determinata da una serie di motivi, variazione dell'impianto informativo, mutate condizioni organizzative o logistiche.

Le modifiche accolte dal responsabile del Sistema Informativo portano alla revisione del GDPR o della Analisi dei rischi. Va ribadito che l'iter di controllo e approvazione dei documenti, di cui ai punti precedenti, deve rispecchiare quello della prima emissione, a meno di cambiamenti del personale

dell'ente o di cambiamenti organizzativi. Per ogni modifica effettuata si aggiorna progressivamente il numero della revisione.
La focalizzazione delle modifiche introdotte con le varie revisioni viene effettuata mediante un segno di evidenziazione del testo. Nel caso di revisione generale, i contenuti della procedura variati sono tali da considerarne una nuova impostazione.
L'aggiornamento dell'archivio cartaceo e di quello elettronico, relativi al PSSI, è compito del Responsabile del sistema informativo.
Quando un Documento della sicurezza è revisionato, il Responsabile della segreteria, conserva la copia superata in formato elettronico in un'apposita directory denominata "Doc_Sicurezza_Superati".
La copia in vigore del Piano di sicurezza, delle Procedure e delle Linee Guida sull'uso delle risorse del sistema informativo sono resi disponibili ai dipendenti del Comune nella intranet aziendale.

Documento	Redazione	Approvazione	Distribuzione	Archiviazione
PSSI/GDPR	Responsabile Ufficio Segreteria	Titolare	Responsabile Ufficio Segreteria	Responsabile Ufficio Segreteria
Procedure	Responsabile Ufficio Segreteria	Titolare	Responsabile Ufficio Segreteria	Responsabile Ufficio Segreteria
Linee Guida sull'Utilizzo delle Risorse Sistema Informativo	Responsabile Ufficio Segreteria	Titolare	Responsabile Ufficio Segreteria	Responsabile Ufficio Segreteria

8 IDENTIFICAZIONE DELLE RISORSE E DELLE INFRASTRUTTURE

Le risorse che in qualche modo intervengono nel trattamento dei dati del titolare sono identificate da:

- Luoghi fisici
- Banche dati
- Apparecchiature
- Personale

Di seguito verrà data una descrizione sommaria di questi elementi.

8.1 Luoghi Fisici

i luoghi fisici dove si svolge il trattamento dei dati sono identificati nel paragrafo capitolo 2

8.2 Sistema Informativo

8.2.1 Server e risorse elaborative

Il sistema informativo del Comune di Romano di Lombardia si compone di una serie di server installati all'interno di locali con accesso selezionato al primo piano rialzato.
Sui server sono installate gli applicativi di gestione dei vari uffici e vengono salvati i file di produttività individuale; L'accesso alle banche dati avviene tramite Rete Locale.
Nella tabella contenuta nell'Allegato1 al presente piano sono identificati i server, il sistema operativo installato e i servizi applicativi e le banche dati presenti sul server.

8.2.2 Networking

La rete LAN è una rete basata su sistema operativo Microsoft.
L'infrastruttura di rete del Comune è costituita da una sala ced, ubicata nell'edificio principale del Comune, in cui sono installati i server del SIC.
Di seguito viene descritta l'infrastruttura di rete del Comune

Infrastruttura di rete
Sede Municipio
Connessione alla rete Internet
Il collegamento alla rete internet attraverso tecnologia in fibra fornita da BTLC e connessione welcome Italia
Apparati di protezione Perimetrale
La rete del Comune è protetta da un firewall che ha funzionalità avanzate di protezione della rete La gestione della rete è fatta attraverso dominio di rete basato active directory Microsoft
Sala CED
Nella locale dei server sono installati gli switch del centro stella che sono collegati con gli armati di rete dislocati ai vari piani Gli apparati di rete del centro stella sono alimentati con batterie di continuità
Apparati di rete ai piani
Ai vari piani degli edifici del Comune possono essere presenti degli armadi di rete nel quale sono installati gli apparati di rete Gli apparati di rete dei piani sono chiusi in armadietti e sono alimentati con delle batterie di continuità
Sede della Biblioteca e degli uffici demografici
La sede della biblioteca e degli uffici demografici sono collegate alla sala server tramite rete in fibra ottica dedicata
Apparati di rete ai piani
Ai piani della sede del Comune possono essere presenti degli armadi nei quali sono installati gli apparati di rete che sono alimentati con delle batterie di continuità
Sede Polizia Locale e Servizi a domanda individuale
La sede della Polizia Locale e degli uffici dei Servizi Sociali sono collegate alla sala server tramite rete in fibra ottica dedicata
Apparati di rete ai piani
Ai piani della sede del Comune possono essere presenti degli armadi nei quali sono installati gli apparati di rete che sono alimentati con delle batterie di continuità

8.2.3 Personal Computer

I PC in dotazione ai collaboratori del Comune sono dotati di sistemi operativi Windows. Su ogni di essi è installato l'antivirus che si aggiorna automaticamente.
L'accesso alle risorse di rete avviene tramite account composto da un identificativo e da una password.
L'aggiornamento del sistema operativo avviene automaticamente
Ogni utente accede al file server in cui vengono salvati i file di office.

8.2.4 Risorse Software

Gli applicativi software utilizzati per il trattamento dei dati sono descritti nell'Allegato 1

8.3 Registro dei Trattamenti

Il registro dei trattamenti descrive le banche dati gestite dal titolare e dai responsabili, ed è riportato nell'Allegato 2
Oltre alle banche dati sono anche identificati i soggetti a cui i dati vengono comunicati, siano essi enti Pubblici o aziende che per conto del Comune svolgono un servizio.
Il registro viene aggiornato dal responsabile dei trattamenti quando viene attivato un nuovo processo che prevede la gestione di banche dati.

9 ANALISI DEI RISCHI

I rischi a cui un sistema è sottoposto possono derivare dall'interno o dall'esterno, essere accidentali o volontari. Questi possono causare la perdita delle informazioni, la loro alterazione, o la non disponibilità.

Tra i possibili fattori di rischio del sistema rientrano:

- Calamità naturali
- Accesso non autorizzato
- Diffusione di software maligno
- Errori nel codice del sw
- Errori nella trasmissione dei dati
- Furti
- Errori umani
- Guasti alle apparecchiature

Una volta identificati i possibili fattori di rischio associato alle diverse parti del Sistema Informatico (asset) è stata descritta la vulnerabilità ed il rischio ad essa associata.
Questo passaggio ha lo scopo di inquadrare i danni che potrebbero essere arrecati alle risorse del sistema.

L'analisi dei rischi è fondamentale per la identificazione le strategie da attuare per prevenire o ridurre il danno.
Un aspetto nell'analisi dei rischi consiste nello stimare le probabilità di accadimento degli eventi indesiderati (dimensione probabilistica).
Questa valutazione è stata fatta dal team di progetto in funzione dell'esperienza delle persone che hanno condotto l'analisi e in relazione alle conoscenze dell'ambiente e del sistema informativo del Comune e tenendo conto delle contromisure adottate dall'ente per mitigare il rischio.

L'ultimo step per la quantificazione del rischio, consiste nel valutare la gravità che questi eventi accidentali possono causare, attuare degli interventi per migliorare la sicurezza del sistema che sono stati riportati nella tabella seguente.
Nel contesto del progetto, la stima degli inconvenienti causata dal verificarsi di certi eventi, non è stata fatta usando un criterio economico. Questo perché molti dei danni che si possono riscontrare sono difficili da quantificare, in quanto legati a disservizi causati ai cittadini o alla perdita di immagine del Comune. Anche in questo caso si è preferito identificare le priorità degli interventi da attuare in base all'esperienza del team di progetto e in funzione delle scelte economico/strategiche dell'ente.

9.1 RISULTATI DELL'ANALISI

Nell'Allegato 3 sono stati evidenziati i risultati dell'analisi condotta presso la sede principale del Comune di Romano di Lombardia

10 PIANO DI SICUREZZA

10.1 Misure organizzative

10.1.1 Nomina del personale incaricato al trattamento dei dati

Nell'ambito del Comune di Romano di Lombardia sono adottati una serie di procedimenti organizzativi volti a migliorare la sicurezza del sistema informativo.
Innanzitutto sono state identificati i ruoli e le responsabilità delle figure professionali che nell'ambito dell'ente trattano dati.
Le figure professionali identificate sono state formalmente incaricate attraverso una delega scritta che identifica competenze e responsabilità relative alla gestione del sistema informativo e al trattamento dei dati.

Le regole di nomina prevedono:

1. Il Titolare Nomina i Responsabili Interni del trattamento dei dati
2. I responsabili Interni incaricano i soggetti che trattano i dati
3. Il titolare o i Responsabili interni nominano i responsabili esterni - fornitori (soggetti che per conto del Comune svolgono servizi che prevedono il trattamento dei dati)

Le strutture all'interno dell'organizzazione complessiva del Comune che si occupano del trattamento di dati personali, anche in relazione ai compiti loro assegnati, sono state individuate in base alla tipologia, all'entità, alla distribuzione e alla organizzazione delle attività svolte all'interno dell'ente.
A tale scopo ciascun dipendente e collaboratore è incaricato ed autorizzato al trattamento dei diversi tipi di dati; gli incarichi - così come la responsabilità per la conservazione dei dati vengono conferiti personalmente al momento dell'inserimento di una nuova figura all'interno della struttura dell'ente;
ciascun incaricato può operare, per il trattamento dei dati, esclusivamente all'interno delle mansioni assegnate e in riferimento alle informazioni ed alle Banche dati disponibili relative alla propria categoria di appartenenza;
Lavoratori a tempo determinato/stagisti/ LSU: i soggetti che trattano dati riferiti all'attività del Comune che, per qualifica attribuita od in relazione alla concreta attività svolta, non rivestono la figura di incaricati, sono stati opportunamente autorizzati al trattamento mediante specifica Nomina (stagisti ecc).

10.1.2 Regole accesso Organi politici e consigliari ai dati trattati

Per quanto riguarda il Consiglio Comunale e la Giunta; tali organi non hanno ruoli diretti di gestione delle banche dati, tuttavia, al fine di svolgere appieno il mandato loro conferito, il sindaco, gli assessori e i consiglieri possono consultare ogni documento, sia cartaceo che informatico, anche contenente dati sensibili;

10.1.3 Società e ditte addette alla Manutenzione degli strumenti di Elaborazione, dei software e delle reti informatiche

Nel caso in cui l'ente richieda l'intervento di ditte specializzate per interventi di assistenza e manutenzione, questi soggetti operano in base a specifica autorizzazione, recante nel dettaglio i compiti da svolgere. In particolare queste Ditte si trovano nella situazione di dover periodicamente svolgere lavori di manutenzione o, semplicemente, di verifica del funzionamento di un programma

o di una attrezzatura informatica. A tal fine è praticamente necessario accedere alle banche dati presenti sui personal computer o all'interno dei programmi software, che si configura come un trattamento ed una conoscenza di dati personali che di per sé non è collegata allo scopo per cui la Ditta effettua la propria attività.
Se l'adozione delle misure di sicurezza viene affidata a soggetti esterni alla propria struttura, quali i fornitori di programmi software dedicati, il Titolare del trattamento riceve dall'installatore una descrizione scritta dell'intervento effettuato e delle operazioni realizzate.

10.2 Audit sulla corretta attuazione dei principi e delle regole di trattamento dei dati

E' stato predisposto un piano di audit per verificare periodicamente la corretta attuazione dei principi e delle misure organizzative e tecniche inerenti il trattamento dei dati e per rivedere l'analisi dei rischi ed il piano delle azioni da implementare per un miglioramento dei processi di gestione delle informazioni. Una sintesi delle attività previste è riportata nel **capitolo 17** del presente documento.
Gli audit sulla compliance al REU 679/2016 sono svolti dal DPO in collaborazione con i Responsabili del trattamento dei dati e con l'amministratore di sistema. Al termine di questa attività viene prodotta una relazione nella quale vengono evidenziati i piani e le attività di miglioramento che il Comune deve adottare (Rapporto di Audit)

10.3 Gestione profili di autorizzazione di accesso al sistema informativo

Nel caso di nuova assunzione o nel caso di variazione dell'organico la procedura (PO-PSI-01) definisce le regole di gestione degli utenti del sistema informativo. La policy prevede la comunicazione, da parte del responsabile dell'area presso la quale il dipendente presta/presterà servizio all'amministratore di sistema, delle variazioni delle mansioni e dei nuovi profili di accesso alle risorse del sistema informativo comunale.
L'amministratore di sistema incaricato dovrà modificare i diritti di accesso alle risorse del sistema informativo e ai dati trattati attraverso strumenti informatici.

10.4 Gestione e comunicazione dell'Informativa

Come previsto dal RE 679/2016 il Comune di Romano di Lombardia ha predisposto dei modelli di informativa rivolti alle diverse categorie di soggetti interessati:

- Cittadini
- Dipendenti del Comune
- Professionisti e dipendenti dei Fornitori

L'informativa è stata esposta, presso i vari uffici e gli sportelli a cui il pubblico accede abitualmente. Per il settore dei servizi sociali, quando si attiva un procedimento che prevede il trattamento di dati relativi allo stato di salute, il documento di informativa viene consegnato al soggetto interessato ed una copia controfirmata viene archiviata nella pratica.
Una comunicazione relativa alle regole e alle modalità di trattamento dei dati è stata esposta sul sito del Comune alla sessione Privacy.
La procedura PO-PSI-04 definisce le regole e le modalità di gestione dell'Informativa e delle modalità con cui acquisire il consenso al trattamento dei dati.

10.5 Gestione delle Comunicazioni e della Pubblicità legale attraverso sito web e l'albo pretorio

La legge n. 69 del 18 giugno 2009, perseguendo l'obiettivo di modernizzare l'azione amministrativa mediante il ricorso agli strumenti informatici riconosce l'effetto di pubblicità legale agli atti e ai provvedimenti amministrativi pubblicati dagli Enti Pubblici sui propri siti informatici.

10.5.1 Pubblicazione on line e rispetto della privacy

Le regole sulla privacy dettate nel Decreto Legislativo n.196 del 2003, che garantiscono il diritto alla tutela dei dati personali sono valide e debbono essere rispettate anche per i siti web (per es. dagli atti pubblicati vanno omessi i dati sensibili ossia quei dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale)
L'albo pretorio contiene diversi provvedimenti che devono essere pubblicati per legge e che possono, a volte, fare menzione di alcuni dati sensibili strettamente indispensabili. Nel predisporre i documenti da affiggere, però, fermo restando il rispetto degli obblighi di legge sulla trasparenza delle deliberazioni adottate, occorre comunque rispettare la riservatezza degli interessati. La pubblicazione indiscriminata di informazioni personali può porsi, infatti, in contrasto con la legge sulla privacy quando ciò non sia necessario al raggiungimento delle finalità per le quali i dati sono stati raccolti.
Con la delibera n.17 del 19 aprile 2007 Allegato1 - Internet: sui siti di comuni e province trasparenza, ma con dati personali indispensabili – Allegato 1: Linee guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione di atti e documenti di enti locali - il garante della privacy consente la diffusione di dati personali per finalità di trasparenza e di comunicazione nelle pubbliche Amministrazioni ma sempre nel rispetto dei principi di pertinenza, non eccedenza e indispensabilità dei dati da pubblicare su internet e pone nuovamente cautele e limiti di fronte alla pubblicazione di dati sensibili che inoltre, richiedono l'adozione di misure di sicurezza per garantire il trattamento dei dati con strumenti elettronici.

10.6 Sicurezza Fisica

La politica della sicurezza identifica i comportamenti che regolano l'accesso fisico a luoghi in cui sono conservati o custoditi dati personali o sensibili. A tale proposito si può identificare una classificazione degli stessi in:

- Aree ad accesso non controllato
- Aree ad accesso controllato
- Aree ad accesso ristretto

Per ognuna di queste sono state definite delle modalità di gestione degli accessi e delle regole per quanto riguarda l'installazione delle apparecchiature.

10.6.1 Controllo degli accessi agli edifici

Le sedi del Comune in cui viene effettuato il trattamento dei dati sono identificate nel capitolo 2 del presente PSSI. Nella tabella sottostante vengono identificati i sistemi di controllo degli accessi ai vari edifici e gli impianti di sicurezza installati

Sede principale	**Sede Municipale**
Indirizzo	Piazza G. Longhi 5
Portierato	Non presente
Video sorveglianza	Attivo sul piazzale antistante l'ingresso della sede comunale
Allarme antintrusione	Impianto allarme volumetrico collegato con vigilanza
Inferriate alle porte o finestre	Non presenti
Vigilanza notturna	Servizio attivato con società di vigilanza
Antincendio	Rilevatori di fumo, estintori, idranti
Accesso all'edificio descrivere	Portone in legno le cui chiavi sono in dotazione al personale dell'ente
Distribuzione chiavi	Tutti i dipendenti che hanno l'ufficio nel palazzo, addetti alle pulizie, polizia locale, LLPP
Sede	**Demografici**
Indirizzo	Piazza XXIV Maggio 1
Portierato	Non presente
Video sorveglianza	Impianto di video sorveglianza che monitora gli ingressi della sede
Allarme antintrusione	Impianto volumetrico
Inferriate alle porte o finestre	Non sono presenti
Vigilanza notturna	Servizio attivato con società di vigilanza
Antincendio	Estintori manutenuti da una ditta specializzata
Accesso all'edificio descrivere	Porte in legno e vetri con maniglioni antipanico
Accesso all'edificio descrivere	porte in legno e vetri con maniglioni antipanico
Distribuzione chiavi registrata	Tutti i dipendenti, addetti alle pulizie, polizia locale, LLPP
Sede	**Biblioteca**
Indirizzo	Piazza XXIV Maggio 1
Portierato	Non presente
Video sorveglianza	Impianto di video sorveglianza che monitora gli ingressi della sede
Allarme antintrusione	Impianto volumetrico
Inferriate alle porte o finestre	Non sono presenti
Vigilanza notturna	Servizio attivato con società di vigilanza
Antincendio	Estintori manutenuti da una ditta specializzata
Accesso all'edificio descrivere	Porte in legno e vetri con maniglioni antipanico
Accesso all'edificio descrivere	porte in legno e vetri con maniglioni antipanico
Distribuzione chiavi registrata	Tutti i dipendenti, addetti alle pulizie, polizia locale, LLPP
Sede	**Polizia locale**
Indirizzo	Via Giacomo Rubini, 24
Portierato	Non presente
Video sorveglianza	controllo ingresso
Allarme antintrusione	Impianto attivo
Inferriate	installate alle finestre presenti
Vigilanza notturna	Servizio attivato con società di vigilanza
Antincendio	Estintori

Accesso all'edificio descrivere	Porte in legno e vetri con maniglioni antipanico con grata in metallo e chiavistello
Distribuzione chiavi registrata	Tutti operatori della polizia locale
Sede	**Servizi alla Persona**
Indirizzo	Via Giacomo Rubini, 24
Portierato	Non presente
Video sorveglianza	Non presente
Allarme antintrusione	Impianto attivo
Inferriate	presenti alle finestre e porte finestre
Vigilanza notturna	Servizio non attivo
Antincendio	Estintori
Accesso all'edificio descrivere	Portone di ingresso in legno con serratura di sicurezza che da sul cortile
Accesso all'edificio descrivere	Uffici Porta ingresso in legno con serratura di sicurezza
Distribuzione chiavi registrata	Chiavi distribuite ai dipendenti dell'ufficio

10.6.2 Aree ad accesso non controllato

Sono quelle aree in cui il pubblico può accedere senza alcuna identificazione o misura di sicurezza. Rientrano in questa categoria:

- la sala del consiglio
- la sala riunioni
- uffici assessori

Regole relative a questi spazi

In queste aree non devono essere installate apparecchiature informatiche contenenti banche dati; non devono essere presenti apparecchiature collegate alla rete del Comune, se le stesse non sono presidiate da un operatore;
non devono essere presenti archivi documentali non adeguatamente protetti.

10.6.3 Aree ad accesso controllato

Sono quelle aree in cui può accedere solamente il personale dipendente dell'ente, nel caso in cui acceda del personale esterno questo deve essere accompagnato da un collaboratore del Comune. In questa tipologia rientrano anche le aree accessibili liberamente al pubblico che durante l'orario di apertura devono essere presidiate dai collaboratori del Comune. Rientrano in queste spazi:

- Uffici del Comune
- Uffici di sportello

Regole relative a questi spazi

Queste aree/uffici al termine dell'orario di lavoro o di chiusura degli sportelli devono essere chiuse al pubblico.
In queste aree possono essere installate apparecchiature informatiche collegate alla rete interna.
Le stazioni di lavoro devono rispettare una serie di misure minime di sicurezza:

- accesso alle risorse del Sistema Informatico attraverso password conosciuta unicamente dall'operatore;

- eventuali apparati di rete devono essere disposti in armadi chiusi.
- gli archivi contenenti banche dati su supporto cartaceo devono essere chiusi a chiave, nel caso siano ubicati nelle aree di permanenza del pubblico.

10.6.4 Aree ad accesso ristretto

Sono quelle aree in cui sono installate apparecchiature critiche quali server, apparati di rete, nonché documenti e banche dati cartacee. L'accesso a tali aree è consentito solamente al personale autorizzato e devono essere all'interno di edifici sotto la responsabilità dell'Amministrazione Comunale.
I locali devono rimanere chiusi e le chiavi custodite dalle persone autorizzate.
L'accesso del personale esterno è regolamentato dal Responsabile.
Le aree ad accesso ristretto identificate presso il Comune di Romano di Lombardia sono essenzialmente:

- la Sala Server
- l'Archivio di Deposito e Storico

Regole di accesso SALA SERVER

Di seguito sono sinteticamente riportati i criteri tecnici ed organizzativi per la protezione delle aree e dei locali interessati alle misure di sicurezza, nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi. Le misure riguardano la sala server del Comune accessibile attraverso una porta dotata di serratura la cui chiave è in dotazione al responsabile dei sistemi informativi.
Un'ulteriore copia delle chiavi è custodita dal responsabile dell'Ufficio Tecnico nel caso si debba accedere alla sala per motivi di emergenza in orari di chiusura degli uffici.

Accesso da parte del personale esterno

Il personale non dipendente che deve accedere al Comune per la manutenzione degli apparati, degli applicativi software o degli impianti, deve registrare l'attività svolta sul registro di controllo degli accessi o attraverso dei rapporti di lavoro, indicando le proprie generalità, data di esecuzione dell'intervento, ed attività eseguito.
Quando delle persone entrano nella Sala server il loro operato è supervisionato da un collaboratore dell'ufficio informatico, che si preoccupa anche di impartire indicazioni inerenti le regole di accesso ai locali.
Nella tabella sottostante sono identificate le misure di protezione fisica della sala server e della sala macchine ubicate nei vari edifici nelle quali sono presenti apparati critici del sistema informativo dell'ente.

Sala Server	Regole Sicurezza
Accesso	Accesso tramite scala che da nella stanza dedicata all'impianto informatico. Sala server dotata di porta
Distribuzione chiavi	Ufficio segreteria e ufficio LLPP
Registro interventi	Attivo
Allarme accesso	Allarme dell'edificio
Antincendio	Estintori manutenuti da una ditta specializzata
Impianto energia elettrica a norma	Controllo messa a terra come da disposizioni normative
Aria condizionata per raffreddamento delle apparecchiature	Impianto attivo
Installazione sistemi UPS	Server ed apparati di rete alimentati da batterie di continuità

Regole di Accesso all'Archivio Comunale storico o di deposito

L'archivio del Comune si distingue in archivio corrente, ed archivio storico.
L'archivio corrente è identificato nelle scaffalature e negli armadi degli uffici del Comune, per i quali verranno identificate delle regole di accesso opportune.
L'archivio storico contiene dati e documenti, ed è ubicato in un locale del Comune a cui possono accedere solamente le persone autorizzate.
L'accesso all'archivio è consentito solo al personale autorizzato, richiedendo la chiave all'ufficio protocollo. E' stato inoltre predisposto un registro M-PSI-21 in cui si devono identificare i documenti prelevati.

Archivio Documentale	Regole Sicurezza
Accesso	Porta con chiave di sicurezza
Distribuzione chiavi	Ufficio segreteria e Ufficio LLPP
Registro prelievi	Definita una procedura per prelievi dei documenti
Allarme accesso	Allarme dell'edificio
Antincendio	Estintori e manichette
Impianto energia elettrica a norma	Impianto elettrico a norma – Vengono fatti controlli periodici della messa a terra

10.6.5 Facility dell'edificio

Di seguito vengono identificate le misure adottate per la gestione della sicurezza e per la prevenzione di eventi naturali dannosi.

Impianto elettrico

L'impianto rispetta la normativa vigente. Eventuali interventi vengono svolti da ditte specializzate.
Periodicamente l'ufficio manutenzione fa un controllo della messa a terra dell'edificio.

Numeri telefonici di emergenza

I numeri telefonici delle ditte che curano l'assistenza hardware e software sono riportati in un elenco appeso nel locale ove sono custoditi il server di rete.

11 REGOLE DI MISURE DI SICUREZZA

In questo paragrafo vengono identificate le politiche per la gestione logica della sicurezza delle informazioni che interessano quindi l'accesso alle basi di dati attraverso gli apparati del sistema informativo.

11.1 Identificazione utenti del sistema informativo

Ogni utente può accedere alla rete del sistema informativo attraverso un identificativo (user id) univoco e password. L'identificativo e la password sono personali.
L'assegnazione dei diritti di accesso alla rete informatica o alla base di dati viene fatta dal responsabile del sistema informativo previa richiesta fatta dal responsabile del trattamento dei dati

11.1.1 Password

La password è assegnata a ciascun utente in forma riservata. Allo stesso è consentito di variarla. La gestione della password prevede una serie di misure sotto riportate atte a rendere efficace l'utilizzo della stessa:
lunghezza minima 8 caratteri;
deve essere sostituita ogni 3 mesi;
non deve essere simile alla precedente;
non deve essere comunicata ai colleghi;
non deve essere annotata su supporti accessibili o leggibili;
non deve contenere termini facilmente riconducibili all'incaricato.

11.1.2 Autenticazione degli utenti

Il sistema informativo prevede due livelli di autenticazione:
autenticazione per accesso alle risorse del sistema. Il Comune di Romano di Lombardia, utilizza i servizi di autenticazione del sistema operativo Windows che prevedono la definizione della lunghezza minima delle password a 8 caratteri e l'utilizzo di una complessità nella definizione del codice di autenticazione.
autenticazione applicativa. Per quanto riguarda gli accessi agli applicativi di business, sono state fornite precise istruzioni ai collaboratori sulla necessità di variare la password secondo le regole sopra indicate. Inoltre, per quelle soluzioni la cui gestione viene fatta da enti esterni, si deve prevedere la creazione di un registro degli utenti come indicato nella procedura PO-PSI-01

11.1.3 Gestione Utenze amministrative

Nell'ambito della gestione della rete del Comune sono state identificati dei soggetti che si occupano della gestione del sistema informativo (amministratori di sistema)
A questi soggetti sono assegnate credenziali di amministratore che devono essere gestite in secondo quanto definito nella circolare AGID n 2-2017.
Le policy di gestione sono le seguenti:

Policy gestione utenze Amministrative	
Identificativo	L'identificativo dell'utenza amministrativa deve fare riferimento ad una persona
Password	La password deve essere di 14 caratteri (rif circolare AGID 2 /2017)

Complessità della Password	La gestione delle parole chiave deve prevedere delle regole di complessità -scadenza ogni tre mesi e non riutilizzo per 3 volte di seguito (rif circolare AGID 2 /2017)
Conservazione delle parole chiave	Le parole chiave devono essere custodite in un luogo sicuro a disposizione del titolare e del responsabile del sistema informativo

11.1.3.1.1 Gestione delle utenze amministrative di soggetti esterni

La gestione del sistema informativo comunale vede la presenza di soggetti esterni quali i fornitori delle applicazioni software usate dagli uffici, soggetti che intervengono nella gestione della rete ecc che per operare devono disporre di utenze amministrative.
La gestione di queste utenze è in carico all'amministratore di sistema del Comune che ha il compito di adottare le seguenti policy:

Policy gestione utenze Amministrative di soggetti esterni	
Permessi	Ad ogni soggetto deve essere assegnata una utenza amministrativa univoca i cui permessi sono limitati all'attività che lo stesso deve svolgere
Identificativo	L'identificativo dell'utenza amministrativa deve fare riferimento ad una persona
Password	La password deve essere di 14 caratteri
Complessità della Password	La gestione delle parole chiave deve prevedere delle regole di complessità
Conservazione delle parole chiave	I soggetti a cui sono assegnate queste utenze amministrative sono registrati in un file a disposizione dell'amministratore interno. Questo consente di tenere traccia dei soggetti a cui sono assegnate e di verificarne l'utilizzo

Le politiche di sicurezza sono descritte nella PO-PSI-01 Gestione utenti del Sistema Informativo

11.1.4 Le regole di autenticazione alla rete del Comune

La gestione dell'assegnazione dei diritti di accesso viene fatta dall'amministratore di Sistema. Nel caso un collaboratore del Comune si dimetta i diritti di accesso devono essere revocati attraverso una comunicazione all'amministratore del sistema da parte dell'ufficio del personale del Comune di Romano di Lombardia. Id e password utilizzate non possono essere associate ad un altro utente.

Variazione incarico

Nel caso in cui il collaboratore ricopra un incarico diverso deve essere fatta una comunicazione al responsabile del sistema informativo il quale provvede a modificare i permessi di accesso alle banche dati e alle risorse del sistema informativo.
La richiesta, deve essere fatta in forma scritta all'Amministratore di Sistema da parte del Responsabile dell'Ufficio che accoglie il dipendente.

Nel caso un'utente del Comune si assenti per un determinato periodo di tempo, il responsabile dei sistemi informativi è in grado di cancellare la password impostata dall'utente e di creare un nuovo id in modo da poter accedere alle risorse del PC.

In modo analogo l'amministratore del sistema è in grado di creare degli utenti temporanei per accedere agli applicativi di business. Per cui la comunicazione delle password in busta chiusa seguirà le regole definite nella PO-PSI-01.

11.1.5 Comunicazione di variazione delle password

Per quegli applicativi e strumenti elettronici il cui accesso è consentito esclusivamente tramite credenziali di autenticazione, la cui gestione e variazione non è riconducibile all'ufficio informatico, la stessa deve essere gestita in forma controllata.
In ogni settore viene identificato un responsabile delle password che gestisce attraverso un registro elettronico o documentale l'elenco dei servizi applicativi esterni al Comune
Nel caso di assenza prolungata dell'incaricato del trattamento dei dati il responsabile dei sistemi informativi o un collaboratore del Comune, previa autorizzazione del responsabile del trattamento, possono utilizzare le credenziali di autenticazione avvertendo l'incaricato dell'intervento effettuato.

11.2 Gestione degli Archivi documentali

Il Comune di Romano di Lombardia gestisce archivi documentali contenenti sia dati personali che sensibili che giudiziari.
Per quanto riguarda la gestione degli archivi cartacei l'ente ha adottato le seguenti regole:
nel caso di documenti archiviati in armadi collocati in luoghi non presidiati dai dipendenti ed accessibili al pubblico, questi devono essere chiusi a chiave in modo da garantire la privacy e l'integrità delle informazioni contenute.
dati personali archiviati in armadi dei vari uffici sono chiusi a chiave, nel caso ciò non sia possibile si provvede a chiudere a chiave l'ufficio.

I **dati sensibili e giudiziari** necessariamente vanno custoditi in armadi dotati di serratura chiudibile a chiave.
Se durante le ore di lavoro, l'operatore del Comune deve accedere ai documenti cartacei contenenti dati relativi ai cittadini del Comune o dati relativi alla gestione dell'ente, gli stessi devono essere gestiti con attenzione in modo da non pregiudicarne la privacy o la sottrazione indebita. Al termine della consultazione gli stessi devono essere riposti con cura negli armadi da cui sono stati prelevati.
Nel caso alcuni documenti contenenti dati personali, sensibili o dati classificati come importanti non siano più utili questi devono essere distrutti in modo da non risultare leggibili.
La gestione dei documenti cartacei compete ai responsabili del trattamento dei dati ognuno per le proprie competenze.

11.2.1 Regole chiusura Uffici ed Armadi

Uffici

- al termine dell'orario di lavoro gli uffici devono essere chiusi; le chiavi sono in possesso ad almeno due persone dell'ufficio ed una depositata presso ufficio manutenzioni.

Armadi (nel caso in cui gli uffici non siano chiudibili): al termine della giornata lavorativa i documenti contenenti dati sensibili vanno riposti negli armadi che devono essere chiusi. Le chiavi sono

depositate in un armadio chiuso, la cui chiave viene custodita secondo le disposizioni del Responsabile dell'ufficio.

11.2.2 Gestione della comunicazione dei dati tramite documenti Cartacei

In questo paragrafo vengono identificate le regole per la trasmissione dei documenti cartacei nell'ambito del Comune di Romano di Lombardia.

Le regole adottate dall'ente prevedono:
le comunicazioni in ingresso vengono protocollate dall'ufficio del protocollo, e i documenti classificati come riservati o contenenti dati sensibili vengono registrati a inoltrati all'ufficio competente come riservati;
nel caso di comunicazioni verso l'esterno, la protocollazione della posta è gestita dai singoli uffici.

Per la trasmissione di documenti tra uffici del Comune, compresi lo smistamento della posta da parte del protocollo, deve rispettare una serie di principi in particolare quello di necessità e pertinenza. Cioè i dati possono circolare solo per ragioni di servizio e per la necessità dei singoli uffici; inoltre la corrispondenza non deve passare indiscriminatamente da più persone evitando passaggi superflui.

11.3 Sicurezza della rete informatica

11.3.1 Attacchi alla sicurezza Informatica

Senza la pretesa di offrire una classificazione formale e completa, possiamo considerare gli attacchi come violazioni delle proprietà di sicurezza precedentemente enunciate. I tipi di attacchi possono essere dunque:

- intercettazioni (violano la proprietà di segretezza dell'informazione);
- alterazioni (violano il requisito di integrità);
- generazioni (violano i requisiti di autenticità e di non-ripudio);
- interruzioni (minacciano la disponibilità del sistema).

Nella tabella sono elencate le caratteristiche principali di ogni categoria di attacco, insieme ad alcuni esempi presi da contesti reali.

11.3.2 Sicurezza della rete

La rete consente alle varie stazioni di lavoro di collegarsi alle unità centrali di elaborazione dei dati. Una rete locale mediante opportuni apparati si può poi collegare ad internet, è intuitivo che i livelli di protezione del sistema informativo cambiano se si verifica quest'ultima condizione.

La rete del Comune di Romano di Lombardia è configurata mediate la definizione di un **Dominio di rete** a cui accedono gli utenti previa autenticazione. Per quanto riguarda la rete locale la politica di gestione degli indirizzamenti prevede l'utilizzo di uno schema di indirizzi IP che utilizzano il servizio DHCP.

Nela tabella di seguito riportata vengono descritte le misure di sicurezza informatica adottate dal Comune

Gestione Rete	
Connessione rete internet	Connessione alla rete di internet attraverso Fibra con linea di Backup
Apparati Protezione perimetrale	Installato firewall Fortigate 51 D content filtering
Strumenti di Protezione perimetrale: IPS	firewall con funzioni IPS
Strumenti di Protezione perimetrale: Antivirus	Non presente
Gli accessi ad internet sono gestiti da un Proxy	Il firewall ha funzioni di filtro dei contenuti e blocca l'accesso a siti che sono stati inseriti in una black list
Viene fatta copia del domain controller	il sever che gestisce il dominio di rete è una macchina virtuale di cui vengono fatte le copie di backup
Configurazione ed installazioni delle Postazioni di lavoro e Server	
Sono presenti server virtualizzati per le installazioni o servizi critici ?	I server critici sono stati virtualizzati e vengono fatte delle copie di sicurezza delle macchine virtuali
Aggiornamento dei sistemi operativi	SERVER: Gli aggiornamenti delle macchine server vengono fatti in base all'importanza e alla criticità della Patch. PDL: sulle postazioni di lavoro è attivo il servizio di aggiornamento in automatico delle PDL
Viene tenuta traccia delle attività di eventuali interventi di manutenzione dei server di rete?	Gli interventi di installazione o manutenzione della rete informatica sono tracciati con dei rapportini di intervento che specificano le attività realizzate da parte di ditte esterne
L'installazione delle postazioni di lavoro viene fatta usando una procedura definita che identifica configurazioni e strumenti di sicurezza da attivare ?	L'installazione delle postazioni di lavoro viene fatta installando un set predefinito di applicazioni software e tool di sicurezza partendo da un'immagine salvata su server
Sono state attivate configurazioni che consentono il ripristino delle Pdl	Nel caso di cattivo funzionamento di una PDL viene fatta la reinstallazione
tool di protezione delle PdL e dei Server	
L'antivirus ha una console di gestione centralizzata che consente di impostare le regole di sicurezza	Symantec end point protection dotato di console centralizzata per la gestione delle singole postazioni di lavoro
Il sw antivirus controlla la presenza di codice maligno quando si collega un dispositivo esterno?	Antivirus controlla i dispositivi esterni quando viene collegato al PC
Regole controllo codice maligno	Controllo in tempo reale, programmazione scansione completa delle postazioni di lavoro impostato durante pausa pranzo a cadenza settimanale

Gestione Rete	
Antivirus controlla se sulla Pdl Vengono installati applicazioni non autorizzate	Funzione non presente
Il fornitore del servizio di posta ha attivato un Servizio Antispam	si
Sulle postazioni di lavoro è stato attivato il Firewall personale	si
Strumenti di Protezione perimetrale: Antispam	Il servizio di posta è protetto da un servizio antispam
Strumenti di monitoraggio della rete	Il comune ha installato un'applicazione software (PRTG) che consente di monitorare il traffico di rete e verificare il corretto funzionamento dei server

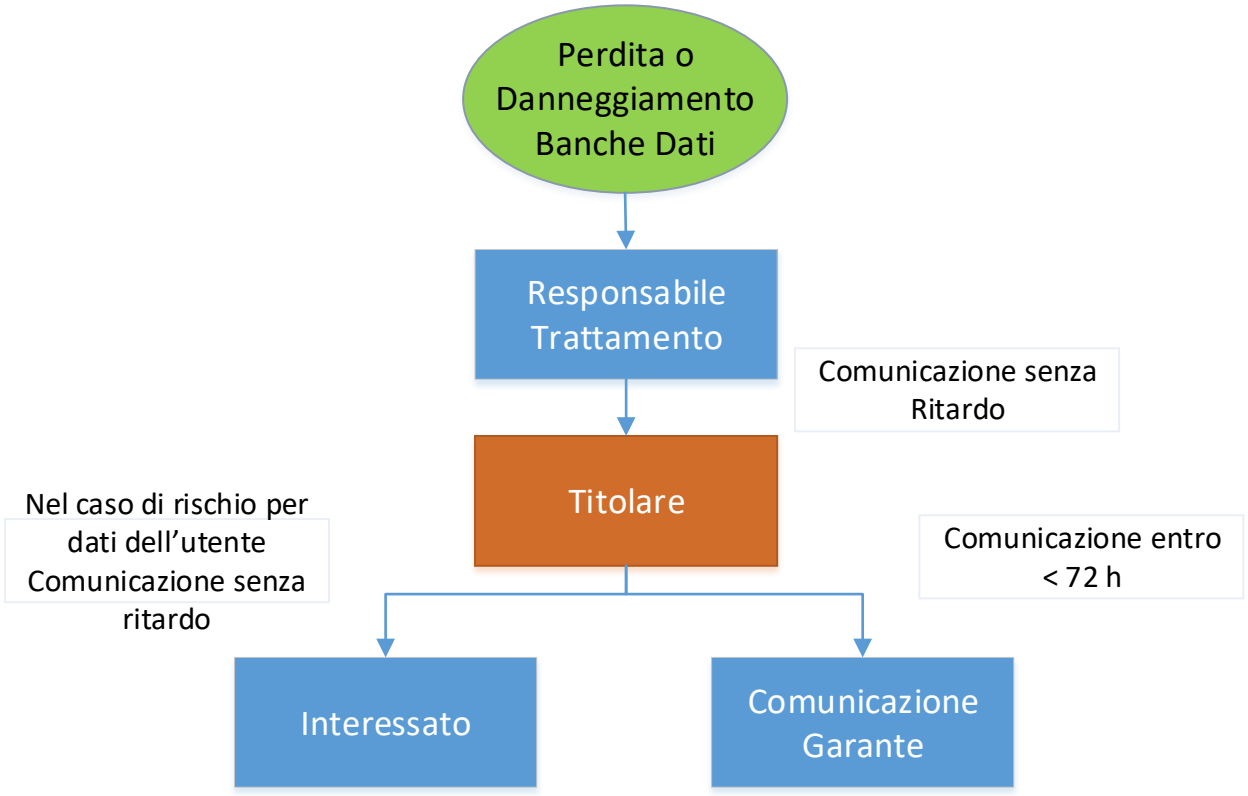
12 VIOLAZIONE O PERDITA DEI DATI

Nel caso in cui ci sia una violazione dei dati personali, intesa come la "violazione della sicurezza che comporta anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ad informazioni personali trasmesse, memorizzate o comunque trattate, l'ente è tenuto a darne comunicazione all'autorità competente.
Entro 72 ore dalla conoscenza del fatto, le amministrazioni pubbliche sono tenute a comunicare al Garante (tramite apposito modello Allegato1 pubblicato sul sito www.garanteprivacy.it) tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali.

La comunicazione deve:

1. descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
2. identificare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
3. descrivere le probabili conseguenze della violazione dei dati personali;
4. descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Inoltre, quando la violazione dei dati personali è suscettibile di danno per i diritti e le libertà delle persone fisiche, il Titolare deve comunicare la violazione anche all'interessato, senza ingiustificato ritardo, descrivendola con un linguaggio semplice e chiaro (salve circostanze al verificarsi delle quali la comunicazione è esclusa). Procedura di dettaglio descritta nella PO-PSI-05



13 FORMAZIONE

La gestione della sicurezza informatica in una qualsiasi organizzazione vede coinvolte in modo stretto gli utenti del sistema. Ciò richiede un piano di formazione rivolto ad ogni dipendente che utilizza le risorse informatiche dell'organizzazione. L'obbiettivo è quello di creare la "cultura della sicurezza" attraverso una serie di attività volte ad illustrare i provvedimenti ed i comportamenti da adottare per migliorare la sicurezza nel trattamento dei dati. Il piano è stato studiato, organizzato e suddiviso sulla base delle specifiche esigenze di ciascuna area in relazione alla natura dei dati trattati e dei rischi generici o specifici che incombono sui dati, nonché dei criteri e delle modalità di evitare tali rischi.

Periodicamente il responsabile dei sistemi informativi del Comune trasmette a tutti i dipendenti del materiale informativo in cui sono riportate le principali regole di gestione ed utilizzo delle risorse del sistema informativo.

13.1 Piano di formazione

Per le risorse umane, che hanno un ruolo chiave nel trattamento di dati personali, è stato fatto un corso di formazione inerente i principi fondamentali del REU 679/2016. I contenuti essenziali del piano di formazione sono:

- ragioni della nuova normativa
- ambito di applicazione materiale e territoriale
- principi generali
- diritti dell'interessato
- titolare e responsabili del trattamento
- data Protection Officer
- obbligo di tenuta di un "Registro delle attività di trattamento" ed effettuazione della "valutazione di impatto sulla protezione dei dati"
- obblighi di consultazione con l'autorità di controllo
- codici di condotta e certificazione
- trasferimento dei dati e problematiche di diritto extracomunitario
- principi legislativi e comunitari
- funzionamento della normativa nell'ambito dei diritti del cittadino
- crimini informatici, frodi, abusi, danni, casistica
- rischi possibili e probabili cui sono sottoposti i dati
- misure di sicurezza tecniche ed organizzative e comportamentali deputate alla prevenzione dei rischi
- comportamenti e modalità di lavoro per prevenire i rischi

Tale formazione viene erogata mediante supporti informativi cartacei, elettronici e/o telematici.

Il piano di formazione verrà erogato anche per i dipendenti neo assunti che nell'ambito delle loro mansioni svolgono un ruolo di responsabili del trattamento dei dati.

14 GESTIONE DEI FORNITORI A CUI SONO ASSEGNATI DEI SERVIZI CHE PREVEDONO IL TRATTAMENTO DI BANCHE DATI

Il Comune di Romano di Lombardia nell'ambito della del proprio operato ha identificato dei soggetti esterni ai quali ha affidato la gestione di alcuni servizi che prevedono il trattamento di banche dati. Questo implica che queste organizzazioni trattano, assumendo decisioni autonome, queste informazioni di cui il Comune è Titolare.
Per ottemperare a quanto previsto dal regolamento europeo in materi di data protection l'ente ha definito una procedura di valutazione e gestione del fornitore PO-PSI-03 nella quale sono definiti i criteri per valutare la capacità dello stesso di gestire in modo corretto queste informazioni:
La procedura prevede alcune fasi che partono dalla definizione di criteri di qualifica, prevedono un processo autorizzativo da parte del titolare a trattare determinate informazioni, e la definizione congiunta con l'ente delle policy per il trattamento dei dati secondo un iter di seguito riassunto:

- Acquisizione di informazioni inerenti le politiche del fornitore in merito alla gestione dei dati
- Definizione di criteri di Selezione del fornitore
- Qualifica del fornitore ed Inserimento dello stesso nell'elenco dei fornitori accreditati
- Autorizzazione del fornitore al trattamento dei dati quale responsabile esterno
- Criteri di sorveglianza dell'operato del fornitore se la gestione dei dati costituisce un processo critico

Rif Procedura Operativa PO-PSI-03

14.1 Qualifica dei Fornitori che trattano dati per conto del Comune

Nel caso in cui l'ente assegni all'esterno dei servizi di competenza del Comune che prevedono il trattamento di dati personali, prima di procedere all'assegnazione dell'incarico devono essere verificare le misure organizzative e tecnologiche attivate in tema di trattamento dei dati.
A tale scopo il responsabile del procedimento invia al fornitore una scheda per la raccolta dei dati sia di carattere generale che inerenti le modalità di gestione delle informazioni.
La scheda presente come allegato alla procedura PO-PSI-03 deve essere restituita al responsabile del procedimento con le informazioni richieste e sottoscritta da parte del rappresentante legale del fornitore.

14.2 Valutazione delle caratteristiche del fornitore

Il responsabile del procedimento unitamente al Responsabile del sistema informativo e al DPO valuta, in funzione della tipologia del servizio che il fornitore deve erogare, se le policy di gestione dei dati sono adeguate al livello di criticità e rischio implicito nel trattamento.
Nel caso siano state riscontrate delle difformità rispetto alle politiche di sicurezza dell'ente viene fatta una comunicazione in cui si chiedono maggiori delucidazioni od un adeguamento agli standard di sicurezza previsti dal Comune e presenti nelle linee guida emanate da AGID.

15 AUDIT DELLA SICUREZZA

15.1 Verifiche generali

Le verifiche sulla corretta applicazione delle misure di sicurezza per la protezione dei dati e delle informazioni gestite dal Comune nel suo complesso e delle misure particolari in riferimento esplicito a quelle previste dalla legge sul trattamento dei dati personali, sono affidate ai Responsabili del trattamento al DPO e al Responsabile dei sistemi informativi che si avvale di apposite liste di controllo. Le singole funzioni sono comunque tenute alle verifiche previste nella tabella di sintesi sotto riportata.

MISURE DA VERIFICARE	OGGETTO DELLE VERIFICHE	CADENZA	RESPONSABILE
Organizzazione			
Aggiornamento GDPR/PSSI	Controlli periodici, ed aggiornamento del PSSI	periodica	DPO
Outsourcing	Verifica criteri di sicurezza dei fornitori	a Campione	Responsabile Trattamento/ DPO
Incarichi inerenti la sicurezza ed il trattamento dei dati	Controlli periodici degli incarichi, dei compiti e delle responsabilità.	periodica	Responsabile Trattamento
Analisi dei rischi	Analisi dei rischi e delle contromisure da adottare per contrastarli.	periodica	Responsabile Trattamento/ DPO
Autorizzazioni all'accesso	Almeno una volta l'anno, è verificata la sussistenza delle condizioni per la loro conservazione	periodica	Amministratore di sistema
Autorizzazioni all'accesso	Rilasciate e revocate periodicamente	costantemente	Amministratore di Sistema
Piano di formazione	Attivazione del piano di formazione per nuovi collaboratori del Comune	periodica	Responsabile Trattamento/ DPO
Protezione fisica			
Protezione delle aree e dei locali	Controlli periodici degli impianti e dei sistemi di sicurezza	periodica	Responsabile servizio manutenzione
Antincendio	Manutenzione periodica secondo le indicazioni dell'installatore	periodica	Responsabile servizio manutenzione
UPS	Manutenzione preventiva UPS Secondo le istruzioni del costruttore.	periodica	Ufficio tecnico
Controllo accessi fisici ai locali	Controlli periodici dei sistemi che regolano l'accesso agli edifici, agli archivi o alle aree ad accesso ristretto.	periodica	Responsabile servizio manutenzione
Protezione Logica			
Criteri e procedure per assicurare l'integrità dei dati	Controlli accessi banche dati. Controllo utilizzo modalità di autenticazione	periodica	Amministratore di Sistema

Codici identificativi personali	Disattivazione in caso di perdita della qualità che consentiva l'accesso all'elaboratore	Sempre	Amministratore di Sistema
Restrizioni di accesso per via telematica	Controllo account sistema informativo	periodica	Amministratore di Sistema
Sicurezza delle trasmissioni dei dati	Controlli periodici log dei firewall	mensile	Amministratore di Sistema
Sistema Informativo			
Misure di sicurezza della rete informatica	Verifica buon funzionamento Verifica aggiornamento	periodica	Amministratore di Sistema
Patching	Aggiornamento periodico dei sistemi informativi dei server Aggiornamento periodico dei sistemi informativi dei client	Ogni mesi	Amministratore di Sistema
Back-up Dati	Verifica back-up dei dati e dei dati di sistema e efficienza apparecchiature e supporti.	Quotidiana	Amministratore di Sistema
Re impiego dei supporti di memorizzazione	Controlli sulla recuperabilità delle informazioni precedentemente contenute	costanteme nte	Amministratore di Sistema

16 Elenco delle Procedure allegate al presente documento

Id Procedura	Descrizione	Responsabile archiviazione
PO-PSI-01	Gestione utenti del sistema informativo	Ufficio Affari Generali
PO-PSI-02	Gestione delle copie di sicurezza dei dati	Ufficio Affari Generali
PO-PSI-03	Gestione dei fornitori a cui sono stati affidati dei trattamenti	Ufficio Affari Generali
PO-PSI-04	Gestione dell'informativa e del consenso al trattamento dei dati	Ufficio Affari Generali
PO-PSI-05	Gestione del Data Breach	Ufficio Affari Generali
PO-PSI-06	Gestione DPIA	Ufficio Affari Generali
PO-PSI-06	Gestione smart Working	Ufficio Affari Generali

COMUNE DI ROMANO DI LOMBARDIA

Data Aggiornamento
22/01/2021

Servizio/Applicativo	Nome del software	Fornitore/Manuten.	Regole di autenticazione applicativa	Regole di gestione
Gestione Biblioteca	Clavis	Rete Bibliotecaria Bergamasca	id e password	Scadenza e complessita
Gestione Demografico	Halley	Halley Informatica Srl	id e password	Scadenza
Gestione Pratiche edilizie	Winedil	Edilsoft srl	id e password	Scadenza
Gestione Presenze	winmark fx client	Basis Srl	id e password	Scadenza
Gestione Personale	Infoline	Infoline Srl	id e password	Scadenza
Gestione Uff Polizia Locale	Concilia	Maggioli SpA	id e password	Scadenza
Gestione Uff Messi	Halley	Halley Informatica Srl	id e password	Scadenza
Gestione Ragioneria	Halley	Halley Informatica Srl	id e password	Scadenza
Gestione Protocollo	Halley	Halley Informatica Srl	id e password	Scadenza
Gestione Segreteria	Halley	Halley Informatica Srl	id e password	Scadenza
Gestione Tributi (IMU - TARI - TASI)	IUC++	Avanced system srl	id e password	Scadenza
Posta elettronica	aruba	Aruba SpA	id e password di rete	Scadenza e complessita
Servizi di portale				
Ufficio Segreteria	Sito web	Iunus Srl	Nessuna autenticazione sito informativo del comune	
Segreteria	Albo Pretorio	Gazzetta Amministrativa Srl	Nessuna autenticazione sito informativo del comune	
Segreteria	Amministrazione trasparente	Gazzetta Amministrativa Srl	Nessuna autenticazione sito informativo del comune	
Ufficio tecnico	SUAP - Sportello	Edilsoft srl	ID e psw e Carta Regionale Servizi	Scadenza e complessita
Ufficio tecnico	SUE - Sportello Telematico	Edilsoft srl	ID e psw e Carta Regionale Servizi	Scadenza e complessita
Ufficio Tributi gestione dei tributi comunali	LinkMate	Avanced system srl	ID e psw e Carta Regionale Servizi	Scadenza e complessita
Gestione dei pagamenti tributi, diritti di segreteria, servizi scolastici	Pago PA	Avanced system srl	ID e psw e Carta Regionale Servizi	Scadenza e complessita

COMUNE DI ROMANO DI LOMBARDIA

Data Aggiornamento 22/01/2021

					Regole Gestione del Back-up					Regole Gestione del Back-up				
Nome Server	**Sistema Operativo / SW Virtualizzazione**	**Software e Servizi**	**Strumenti Protezione Sicurezza**	**Ubicazione**	**Frequenza backup**	**periodo conservazione**	**sw gestione backup**	**Unità di salvataggi**	**Ubicazione NAS**	**Frequenza backup**	**periodo conservazione**	**sw gestione backup**	**Unità di salvataggi**	**Ubicazione NAS**
Esxi05	VMware Vsphere I	sistema virtualizzazione	Dischi RAID- doppia Scheda di rete - due alimentatori	Sala Server										
DC03	SRV virtuale - Windows 2012	Controllo di dominio	Dischi RAID	Sala Server	incrementale giornaliera ful fine settimana	2 settimane	veeam	NAS01	sala server	incrementale giornaliera ful fine settimana	2 settimane	veeam	NAS02	Biblioteca
PROTOCOLLO	SRV virtuale - Windows 2012	Vecchio server protocollo per sola consultazione	Dischi RAID	Sala Server	incrementale giornaliera ful fine settimana	2 settimane	veeam	NAS01	sala server	incrementale giornaliera ful fine settimana	2 settimane	veeam	NAS02	Biblioteca
APPLSRV03	SRV virtuale - Windows 2016	Server anagrafe, ragioneria, segreteria e repository atti amministrativi (applicativo Halley)	Dischi RAID	Sala Server	incrementale giornaliera full fine settimana	2 settimane	veeam/windows image backup	NAS01	sala server	incrementale giornaliera full fine settimana	2 settimane	veeam/windows image backup	NAS02	Biblioteca
APPLSRV04	SRV virtuale - Windows 2016	Edilsoft	Dischi RAID	Sala Server	incrementale giornaliera full fine settimana	2 settimane	veeam/windows image backup	NAS01	sala server	incrementale giornaliera full fine settimana	2 settimane	veeam/windows image backup	NAS02	Biblioteca
Server Centralino	SRV virtuale - Windows XP	AW per gestione centrale telefonica	Dischi RAID	Sala Server	incrementale giornaliera full fine settimana	1 settimana	veeam	NAS01	sala server	incrementale giornaliera full fine settimana	1 settimana	veeam	NAS02	Biblioteca
Server Mozart	SRV virtuale - Windows 2003	Server virtuale timbrature	Dischi RAID	Sala Server	incrementale giornaliera full fine settimana	1 settimana	veeam	NAS01	sala server	incrementale giornaliera full fine settimana	1 settimana	veeam	NAS02	Biblioteca
NagiosSrV	SRV virtuale - Linux	SW NAGIOS :monitoraggio di computer e risorse di rete	Dischi RAID	sede polizia Locale	full fine settimana	1 settimana	veeam	NAS01	sala server	full fine settimana	1 settimana	veeam	NAS02	Biblioteca
Esxi06	VMware Vsphere II	sistema virtualizzazione	Dischi RAID- doppia Scheda di rete - due alimentatori	Sala Server										
DC02	SRV virtuale - Windows 2016	Controllo di dominio	Dischi RAID	Sala Server	incrementale giornaliera ful fine settimana	2 settimane	veeam	NAS01	sala server	incrementale giornaliera ful fine settimana	2 settimane	veeam	NAS02	Biblioteca
APPLSRV02	SRV virtuale - Windows 2016	Cartelle degli utenti con accesso profilato	Dischi RAID	Sala Server	incrementale giornaliera full fine settimana	2 settimane	veeam/windows image backup	NAS01	sala server	incrementale giornaliera full fine settimana	2 settimane	veeam/windows image backup	NAS02	Biblioteca
SRVArchivio	SRV virtuale - Windows 2000	Vecchio sistema protocollo antecedente Datagraf	Dischi RAID	Sala Server	incrementale giornaliera full fine settimana	2 settimane	veeam/windows image backup	NAS01	sala server	incrementale giornaliera full fine settimana	2 settimane	veeam/windows image backup	NAS02	Biblioteca
Carabinieri	SRV virtuale - Windows XP	connessione con Carabinieri per AOL	Dischi RAID	Sala Server	incrementale giornaliera full fine settimana	2 settimane	veeam/windows image backup	NAS01	sala server	incrementale giornaliera full fine settimana	2 settimane	veeam/windows image backup	NAS02	Biblioteca
VM-S7	SRV virtuale - Windows XP	software pensioni S7	Dischi RAID	Sala Server	incrementale giornaliera full fine settimana	2 settimane	veeam/windows image backup	NAS01	sala server	incrementale giornaliera full fine settimana	2 settimane	veeam/windows image backup	NAS02	Biblioteca
Server video sorveglianza	VMware Vsphere III	sistema virtualizzazione	Dischi RAID- doppia Scheda di rete - due alimentatori	Sala Server										
Srv-Lettura Targhe	VMware Vsphere III	server virtuale per lettura targhe		sede polizia Locale										
Srv-Lettura Targhe	VMware Vsphere III	server virtuale per lettura targhe per gestione ZTL - Dopo 1 mese importate in Concilia		sede polizia Locale										
Srv-Lettura Video sorv	VMware Vsphere III	Server virtualeVideo sorveglianza comunale		sede polizia Locale										

/
/