Comune di Parma

POLITICA DI SICUREZZA INFORMATICA E PER LA SICUREZZA DELLE INFORMAZIONI

Documento per approvazione formale ai fini GV.PO-01

Questo documento è confidenziale. Le informazioni confidenziali non devono essere divulgate a terze parti diverse dai dipendenti e dai fornitori autorizzati da Comune di Parma e IT.CITY con apposita autorizzazione scritta. Le terze parti autorizzate potranno solo prendere visione della versione cartacea o digitale del documento presso le sedi del Comune di Parma e di IT.CITY. Le informazioni confidenziali devono essere tenute in luogo sicuro e non devono essere riprodotte o usate per scopi non autorizzati da Comune di Parma e IT.CITY. La riproduzione può avvenire solo con l'autorizzazione del Comune di Parma e di IT.CITY e le copie devono recare la classificazione dei documenti originali.
I documenti originali sono conservati e consultabili nel repository documentale sharepoint Settore Transizione Digitale - Pagina iniziale).

Redazione, Variazioni, Approvazioni

Redazione

Autore:
Data di creazione: 15/02/2026
Ultimo aggiornamento: 03/06/2026
Codice: Politica di Sicurezza delle Informazioni
Versione: 1.1
Stato:
Classificazione: PUBBLICO

Variazioni

Data	Autore	Versione	Variazione
03/06/2026	Settore Sviluppo Economico e Transizione Digitale	1.1	Adeguamento ISO/IEC 27001:2022 e NIS2 (D.Lgs. 138/2024)

Approvazioni

Nome	Funzione	Data	Firma
Nicola Ferioli	Dirigente Settore Sviluppo Economico e Transizione Digitale	29/06/2026	

Lista distribuzione

L'elenco delle risorse che accedono al documento è gestito. Il documento è accessibile all'interno di un repository.

IT.CITY S.P.A. (Società in house, controllata – a socio unico – sottoposta all'attività di direzione e coordinamento del Comune di Parma) tramite contratto stipulato in data 23 maggio 2022 Rep. N. 19608 della Raccolta Scritture Private del Comune di Parma, maggio 2022 - aprile 2025, e rinnovato fino ad aprile 2028 mediante la stipula del contratto Rep. SP/20365/2025 del 4 luglio 2025, è stata nominata Gestore del Sistema Informatico Comunale di Parma. Il presente documento, ai sensi del Contratto sopracitato, garantisce lo sviluppo coerente e l'integrazione di nuove tecnologie nell'intero sistema informativo dell'Ente e definisce le procedure e le istruzioni sicurezza per una gestione efficace e completa.

SOMMARIO

1. INTRODUZIONE 5
2. SCOPO E CAMPO DI APPLICAZIONE 5
3. RIFERIMENTI NORMATIVI E DOCUMENTALI 6
4. CONTENUTO DELLA POLITICA 6
5. LINEE GUIDA DELLA POLITICA 7
6. RUOLI E RESPONSABILITA' 8
7. MISURE DI SICUREZZA 9
7.1 Gestione del rischio 10
7.2 Classificazione delle informazioni 10
7.3 Sicurezza della catena di fornitura (Supply Chain) 10
8. RISCHI ED OPPORTUNITÀ DEL MODELLO DI GESTIONE DELLA SICUREZZA 11
8.1 Rischi 11
8.2 Opportunità 11
9. OBIETTIVI DEL MODELLO DI GESTIONE DELLA SICUREZZA 11
10. FRAMEWORK DOCUMENTALE 12
10.1 Framework documentale SGSI di IT.CITY S.p.A. 12
10.2 Framework documentale specifico del Comune di Parma 13

1. INTRODUZIONE

La presente Politica per la Sicurezza delle Informazioni costituisce il documento di indirizzo strategico dell'Ente in materia di sicurezza delle informazioni e di sicurezza informatica (cybersecurity). Ai fini della presente politica, la sicurezza informatica rappresenta una componente della più ampia sicurezza delle informazioni ed è finalizzata alla protezione delle informazioni, dei sistemi informativi, delle reti e dei servizi digitali mediante l'adozione di misure organizzative, tecniche e procedurali.

La Politica definisce i principi e gli obiettivi per la tutela della riservatezza, dell'integrità, della disponibilità e dell'autenticità del patrimonio informativo dell'Ente, in conformità alla normativa vigente e agli indirizzi dell'Agenzia per la Cybersicurezza Nazionale.

Eventuali compromissioni della sicurezza delle informazioni o interruzioni dei servizi digitali possono determinare impatti significativi sull'operatività dell'Ente e sui servizi erogati alla collettività. In tale prospettiva, le Pubbliche Amministrazioni rivestono un ruolo essenziale nell'ambito della sicurezza informatica e della resilienza delle infrastrutture critiche nazionali.

La presente Politica si inserisce nel quadro delle azioni intraprese dall'Ente per garantire la conformità al Decreto Legislativo 4 settembre 2024, n. 138, di recepimento della Direttiva (UE) 2022/2555 (NIS2).

Il Comune di Parma adotta un proprio modello organizzativo e di governo per la gestione della sicurezza delle informazioni e della cybersicurezza, nell'ambito del quale sono definiti ruoli, responsabilità, autorità e funzioni di indirizzo, governo, supervisione e controllo.

Per l'attuazione operativa di tale modello, il Comune si avvale del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) adottato da IT.CITY S.p.A., società in house dell'Ente, nonché delle relative politiche, procedure, metodologie e misure di sicurezza, per quanto applicabili ai servizi affidati e al perimetro comunale.

Restano in capo al Comune di Parma la governance complessiva della sicurezza, l'indirizzo strategico, il governo e l'accettazione del rischio, l'approvazione delle misure e dei piani di propria competenza, la supervisione e la vigilanza sulla loro attuazione, in conformità al Decreto Legislativo 4 settembre 2024, n. 138 e alle altre disposizioni applicabili in materia di cybersicurezza.

2. SCOPO E CAMPO DI APPLICAZIONE

La presente Politica definisce i principi, gli obiettivi e gli indirizzi generali adottati dal Comune di Parma per garantire la sicurezza delle informazioni e la cybersicurezza, mediante l'istituzione, il mantenimento e il miglioramento continuo del proprio modello organizzativo e di governo

La Politica è finalizzata a:

- garantire la riservatezza, l'integrità, la disponibilità e l'autenticità delle informazioni;
- assicurare la protezione dei sistemi informativi, delle reti, delle infrastrutture digitali e dei servizi ICT;

- assicurare la valutazione, il trattamento, il monitoraggio e il governo dei rischi relativi alla sicurezza delle informazioni e alla cybersicurezza;
- assicurare la conformità ai requisiti normativi, regolamentari e contrattuali applicabili;
- promuovere la diffusione della cultura della sicurezza e della consapevolezza del personale;
- contribuire alla continuità operativa e alla resilienza dei servizi erogati dall'Ente.

La presente Politica si applica:

- a tutte le informazioni trattate dal Comune di Parma, indipendentemente dal formato o dal supporto utilizzato (digitale, cartaceo);
- ai sistemi informativi, alle reti, alle applicazioni, alle piattaforme digitali e alle infrastrutture tecnologiche utilizzate per l'erogazione dei servizi dell'Ente;
- a tutti i dipendenti, dirigenti, amministratori, collaboratori, consulenti, fornitori e soggetti terzi che, a qualsiasi titolo, accedono o trattano informazioni o utilizzano risorse informative riconducibili all'Ente;
- ai processi organizzativi e ai servizi che comportano il trattamento di informazioni e l'utilizzo di sistemi informativi.

L'attuazione operativa della presente Politica è assicurata attraverso la documentazione specifica del Comune di Parma e, attraverso le politiche, le procedure, gli standard e le misure di sicurezza del SGSI di IT.CITY S.p.A. applicabili al perimetro dell'Ente. Restano in capo al Comune di Parma le funzioni di indirizzo, governo, approvazione, supervisione e controllo, nonché le responsabilità previste dalla normativa vigente.

3. RIFERIMENTI NORMATIVI E DOCUMENTALI

- Codice dell'Amministrazione Digitale (CAD)
- Serie di standard ISO/IEC 27000:2018 - Sicurezza e Gestione delle Informazioni
- Standard ISO/IEC 27001:2022 - Sistema di Gestione della Sicurezza delle Informazioni (SGSI)
- Standard ISO/IEC 27002:2022 - Controlli di sicurezza delle informazioni e cybersecurity
- Standard ISO/IEC 27005:2022 - Gestione dei rischi di sicurezza delle informazioni
- D.Lgs. 196/2003 - codice in materia di protezione dei dati personali aggiornato con D.Lgs. 101/2018 per adeguamento al Regolamento Europeo 679/2016 (GDPR)
- D.Lgs. 138/2024 - recepimento della Direttiva (UE) 2022/2555 NIS2
- Provvedimenti e Autorizzazioni Generali dell'Autorità Garante e qualsiasi altra norma applicabile avente ad oggetto il trattamento di dati personali
- Contratto di Servizio per la gestione del sistema informativo tra Comune di Parma ed IT City SPA.
- Determinazione del Direttore generale dell'ACN (Agenzia per la Cybersicurezza Nazionale) n. 164179 del 14 aprile 2025 – Allegato 1 "Misure di sicurezza di base per i soggetti importanti"
- Normativa in materia del diritto d'autore (legge 633 del 1941 e s.m.)

4. CONTENUTO DELLA POLITICA

La presente Politica rappresenta il documento di indirizzo del modello organizzativo adottato dal Comune di Parma per la sicurezza delle informazioni e la cybersicurezza. Essa definisce i principi che devono orientare le decisioni dell'Ente e l'attuazione delle misure organizzative, procedurali,

fisiche e tecnologiche, comprese quelle realizzate da IT.CITY S.p.A. e dagli altri soggetti affidatari nell'ambito delle rispettive competenze.

La presente Politica definisce i principi generali per la protezione delle informazioni, dei sistemi informativi, delle reti, delle infrastrutture tecnologiche e dei servizi digitali utilizzati dal Comune di Parma.

La sicurezza delle informazioni è perseguita attraverso l'adozione di misure tecniche, organizzative e procedurali proporzionate ai rischi individuati e integrate nei processi dell'Ente, al fine di garantirne l'efficace applicazione e il miglioramento continuo.

In particolare, il modello organizzativo del Comune di Parma per la sicurezza delle informazioni e la cybersicurezza si fonda sui seguenti principi:

:

- identificazione e valutazione periodica dei rischi per la sicurezza delle informazioni e dei servizi digitali;
- definizione e attuazione di adeguate misure di protezione e mitigazione;
- monitoraggio e verifica dell'efficacia dei controlli di sicurezza adottati;
- gestione degli incidenti di sicurezza e delle situazioni di crisi informatica;
- promozione della consapevolezza e della formazione del personale;
- miglioramento continuo del modello organizzativo, delle misure di sicurezza e della postura di sicurezza dell'Ente.

5. LINEE GUIDA DELLA POLITICA

Il Comune di Parma riconosce la sicurezza delle informazioni quale elemento essenziale per l'erogazione dei servizi istituzionali, la tutela dei dati trattati e il mantenimento della fiducia di cittadini, imprese e altri portatori di interesse.

A tal fine, l'Ente si impegna a:

- garantire la riservatezza, l'integrità, la disponibilità e l'autenticità delle informazioni trattate;
- adottare un approccio basato sulla valutazione e gestione del rischio per la sicurezza delle informazioni e la cybersicurezza;
- assicurare la conformità alle disposizioni normative, regolamentari e contrattuali applicabili;
- proteggere le informazioni durante l'intero ciclo di vita, dalla creazione alla conservazione, dall'utilizzo alla trasmissione, fino alla cancellazione o distruzione;
- assicurare che l'accesso alle informazioni e alle risorse informatiche avvenga secondo il principio del minimo privilegio e in funzione delle effettive esigenze operative;
- promuovere la formazione e la consapevolezza del personale in materia di sicurezza delle informazioni e cybersicurezza;
- garantire la gestione tempestiva degli incidenti di sicurezza e delle situazioni di crisi informatica;
- assicurare che fornitori, partner e soggetti terzi adottino adeguate misure di sicurezza in relazione ai servizi erogati e alle informazioni trattate per conto dell'Ente.

- garantire che i rischi derivanti dalla catena di fornitura ICT, dai fornitori, dai partner tecnologici e dai servizi esternalizzati siano identificati, valutati, monitorati e trattati nell'ambito del processo di gestione del rischio dell'Ente
- monitorare periodicamente l'efficacia delle misure adottate e perseguire il miglioramento continuo del modello organizzativo comunale e, per gli ambiti applicabili, dei processi e dei controlli attuati attraverso il SGSI di IT.CITY S.p.A.

Tutte le informazioni trattate dal Comune di Parma devono essere adeguatamente protette in funzione della classificazione attribuita e del livello di rischio associato. Le informazioni devono essere gestite in modo sicuro, accurato, affidabile e rese disponibili ai soggetti autorizzati quando necessario per lo svolgimento delle attività istituzionali.

6. RUOLI E RESPONSABILITA'

Ruoli e responsabilità sono definiti nel documento "ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA - RUOLI E RESPONSABILITA' PER LA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI".

Le responsabilità di indirizzo, governo, approvazione, supervisione e controllo sono attribuite agli Organi di amministrazione e direttivi del Comune di Parma, secondo le rispettive competenze e in conformità alla normativa.

Gli Organi di Amministrazione e Direttivi definiscono gli obiettivi di sicurezza, assicurano un indirizzo chiaro e coerente con le strategie dell'Ente, garantiscono un supporto visibile alle iniziative in materia di sicurezza delle informazioni e cybersicurezza e promuovono la disponibilità di risorse adeguate, assicurando la congruità dei budget destinati alla sicurezza. Essi approvano formalmente la presente Politica, ne assicurano la comunicazione e l'applicazione nell'ambito dell'Ente e ne verificano periodicamente l'adeguatezza rispetto agli obiettivi dell'Ente, all'evoluzione del contesto normativo, organizzativo e tecnologico e agli esiti delle attività di monitoraggio, audit e riesame.

In applicazione del D.Lgs. 138/2024, gli Organi di amministrazione e direttivi approvano le modalità di attuazione delle misure di gestione del rischio, ne sovrintendono l'attuazione e ricevono informazioni periodiche sulla postura di sicurezza, sui rischi e sullo stato delle misure, nonché informazioni tempestive sugli incidenti significativi e sulle relative notifiche. Le responsabilità di indirizzo, approvazione, supervisione e vigilanza restano in capo al Comune anche quando l'esecuzione operativa sia affidata a IT.CITY S.p.A. o ad altri fornitori.

Fermo restando il riparto formale delle competenze, i componenti degli Organi rispondono anche personalmente delle violazioni degli obblighi loro attribuiti, nei limiti e secondo il regime previsto dal decreto e dall'ordinamento applicabile.

La formazione specifica e periodica in materia di sicurezza informatica è obbligatoria per i componenti degli Organi di Amministrazione e Direttivi; il Piano di Formazione definisce contenuti, periodicità ed evidenze. La puntuale attribuzione delle competenze tra Sindaco, Giunta, Segretario Generale, RTD e altri soggetti competenti è formalizzata dall'Ente

Il RTD, con il Punto di Contatto ACN e il relativo sostituto, presidiano gli adempimenti previsti sulla piattaforma ACN, nei termini normativi, come ad esempio la registrazione annuale e l'aggiornamento dei dati del Comune.
L'attuazione operativa e il coordinamento delle attività sono demandati alle funzioni e ai ruoli individuati.

Tutto il personale, nonché i soggetti che operano per conto dell'Ente, è tenuto a rispettare la presente Politica, le procedure e le misure di sicurezza applicabili, contribuendo alla protezione delle informazioni e segnalando tempestivamente eventi, anomalie, vulnerabilità o incidenti di sicurezza di cui venga a conoscenza.

RISORSE PER LA GESTIONE E IL MIGLIORAMENTO DELLA SICUREZZA DELLE INFORMAZIONI

Il Comune di Parma assicura, nell'ambito delle proprie competenze, la disponibilità delle risorse organizzative, professionali, tecnologiche ed economiche necessarie al funzionamento e al miglioramento del proprio modello organizzativo per la sicurezza delle informazioni e la cybersicurezza.

Le risorse necessarie al perseguimento degli obiettivi di sicurezza delle informazioni sono individuate e riesaminate periodicamente dagli Organi di Amministrazione e Direttivi dell'Ente, tenendo conto dell'evoluzione del contesto organizzativo, dei rischi per la sicurezza delle informazioni, delle esigenze operative e degli indirizzi strategici definiti.

L'adeguatezza delle risorse è oggetto di monitoraggio periodico nell'ambito delle attività di governo e riesame, al fine di garantirne l'efficacia e il miglioramento continuo.

7. MISURE DI SICUREZZA

La gestione della sicurezza delle informazioni si fonda sull'adozione di un insieme strutturato e documentato di misure organizzative, procedurali e tecnologiche finalizzate a prevenire, ridurre e gestire i rischi che possono incidere sulla riservatezza, sull'integrità e sulla disponibilità delle informazioni e dei servizi dell'Ente. Tali misure sono definite secondo un approccio basato sul rischio e sono soggette a monitoraggio e miglioramento continuo.

L'attuazione della presente Politica tiene conto del ciclo di gestione previsto dalle clausole 4-10 della ISO/IEC 27001:2022, comprendente l'analisi del contesto e delle parti interessate, la leadership, la pianificazione basata sul rischio, la disponibilità di risorse e competenze, il controllo operativo, la valutazione delle prestazioni e il miglioramento.

Le misure sono proporzionate al rischio e comprendono almeno: analisi dei rischi e sicurezza dei sistemi; gestione e notifica degli incidenti; continuità operativa, backup, disaster recovery e crisi; sicurezza della catena di fornitura; sicurezza nell'acquisizione, sviluppo e manutenzione; valutazione dell'efficacia; igiene informatica e formazione; crittografia; sicurezza delle risorse umane, controllo degli accessi e gestione degli asset; autenticazione a più fattori e comunicazioni sicure.

Viene assicurata inoltre la copertura esplicita dei controlli ISO/IEC 27001:2022 Annex A / ISO/IEC 27002:2022 A.5.7 Threat intelligence, A.5.23 Sicurezza dei servizi cloud, A.5.30 Prontezza ICT per la continuità operativa, A.7.4 Monitoraggio della sicurezza fisica, A.8.9 Gestione della configurazione, A.8.10 Cancellazione delle informazioni, A.8.11 Data masking, A.8.12 Prevenzione della perdita di dati,

A.8.16 Attività di monitoraggio, A.8.23 Web filtering e A.8.28 Codifica sicura, ove applicabile. L'attuazione di dettaglio è rinviata ai documenti specialistici e tracciata nel Piano di Adeguamento/Trattamento.

7.1 Gestione del rischio

Il Comune di Parma adotta un approccio integrato alla resilienza organizzativa, assicurando il coordinamento tra la Procedura di gestione degli incidenti di sicurezza delle informazioni, il Piano di gestione delle crisi, il Piano di trattamento del rischio, il Piano di continuità operativa e il Piano di disaster recovery dell'Ente.

Le misure di sicurezza e le azioni di adeguamento previste dalla documentazione comunale sono correlate, ove applicabile, agli scenari individuati nell'ambito del processo di valutazione e trattamento del rischio del Comune di Parma.

7.2 Classificazione delle informazioni

Le informazioni del Comune di Parma sono classificate secondo quanto previsto dal Regolamento Generale sulla Protezione dei Dati GDPR EU 2016/679, Codice in materia di protezione dei dati personali.

IT.CITY S.p.A. tratta i dati personali per conto del Comune di Parma negli ambiti definiti dagli atti di affidamento e dagli accordi applicabili, adottando le misure tecniche e organizzative di propria competenza. Restano ferme le responsabilità del Comune di Parma quale titolare del trattamento e quelle degli altri soggetti individuati dalla normativa in materia di protezione dei dati personali.

Tutte le informazioni e i dati trattati sono protetti mediante l'applicazione delle migliori misure di sicurezza tecniche e organizzative disponibili e adottate dall'Ente e da IT.CITY, indipendentemente dalla loro tipologia, nel rispetto dei principi di riservatezza, integrità e disponibilità.

7.3 Sicurezza della catena di fornitura (Supply Chain)

Il Comune di Parma riconosce che la sicurezza delle informazioni dipende anche dall'affidabilità e dalla sicurezza dei fornitori, dei partner tecnologici e dei soggetti esterni che, a qualsiasi titolo, forniscono beni, servizi o soluzioni che possono avere impatto sui sistemi informativi, sui dati trattati o sulla continuità dei servizi dell'Ente.

Il Comune adotta un approccio basato sul rischio per la gestione della sicurezza della catena di fornitura ICT e dei servizi esternalizzati, assicurando che i rischi derivanti da fornitori, subfornitori e terze parti siano identificati, valutati, monitorati e trattati in modo proporzionato alla criticità dei servizi e delle informazioni coinvolte.

Nell'ambito della propria organizzazione, il Comune di Parma si avvale di IT.CITY S.p.A., società in house, per l'erogazione di specifici servizi ICT e di cybersicurezza. Il Comune può altresì affidare direttamente beni e servizi ad altri fornitori qualificati, secondo le procedure previste dalla normativa vigente. In tutti i casi, i requisiti di sicurezza e le attività di controllo sono definiti e applicati secondo criteri coerenti con il modello organizzativo e i requisiti di sicurezza del Comune di Parma.

.

La gestione dei rischi della supply chain, indipendentemente dalla modalità di affidamento dei servizi, costituisce parte integrante del processo di gestione del rischio dell'Ente ed è oggetto di monitoraggio e riesame periodico.

Il Comune di Parma assicura che i fornitori, i partner tecnologici e gli altri soggetti esterni che accedono a informazioni, sistemi o servizi dell'Ente siano tenuti al rispetto di requisiti di sicurezza coerenti con il Sistema di Gestione per la Sicurezza delle Informazioni (SGSI), con la normativa applicabile e con il livello di rischio associato ai servizi erogati. Tali requisiti comprendono specifiche clausole contrattuali, obblighi di riservatezza, requisiti di continuità operativa, misure di protezione delle informazioni, obblighi di segnalazione degli incidenti e attività di verifica e monitoraggio periodico. In caso di affidamento di servizi critici o rilevanti ai fini della sicurezza delle informazioni, il Comune può richiedere ulteriori evidenze, attestazioni o garanzie in materia di sicurezza informatica e resilienza operativa.

Per i servizi ICT, cloud e di sviluppo software, le clausole contrattuali includono, ove applicabile, requisiti di secure-by-design e secure coding, gestione delle vulnerabilità, controllo delle modifiche e delle configurazioni, protezione dei dati, continuità operativa, diritto di audit, gestione dei subfornitori e notifica a cascata degli incidenti in tempi compatibili con gli obblighi del Comune verso CSIRT Italia e ACN.

8. RISCHI ED OPPORTUNITÀ DEL MODELLO DI GESTIONE DELLA SICUREZZA

8.1 Rischi

I rischi che possono influire sul conseguimento degli obiettivi di sicurezza e sull'efficacia del modello organizzativo comunale sono identificati, monitorati, riesaminati e gestiti mediante adeguate azioni di trattamento. L'efficacia delle azioni è valutata nell'ambito delle attività di monitoraggio, verifica, riesame e miglioramento continuo.

8.2 Opportunità

Le opportunità di miglioramento sono identificate, valutate e riesaminate periodicamente al fine di incrementarne l'efficacia, rafforzare la sicurezza delle informazioni e favorire il miglioramento continuo del sistema.
Le opportunità possono derivare, tra l'altro, dall'evoluzione normativa, dall'innovazione tecnologica, dagli esiti delle attività di audit, dall'analisi degli incidenti e dall'accrescimento delle competenze del personale
La conformità è verificata mediante monitoraggio, audit, riesame della direzione, indicatori di efficacia e gestione delle non conformità. L'Ente mantiene evidenze idonee a supportare eventuali attività di vigilanza e ispezione dell'ACN e considera il regime sanzionatorio previsto dal D.Lgs. 138/2024. Il presente richiamo non costituisce parere legale; l'interpretazione definitiva è rimessa al RTD e alla funzione legale interna.

9. OBIETTIVI DEL MODELLO DI GESTIONE DELLA SICUREZZA

L'obiettivo è garantire un livello adeguato di protezione delle informazioni, dei sistemi informativi e dei servizi digitali dell'Ente, attraverso l'identificazione, la valutazione e il trattamento dei rischi che possono comprometterne la sicurezza, la continuità e la resilienza.

A tal fine, viene definito e coordinatol'insieme delle misure organizzative, tecniche e procedurali necessarie a garantire il conseguimento dei seguenti obiettivi fondamentali di sicurezza:

- **RISERVATEZZA**: le informazioni devono essere accessibili esclusivamente ai soggetti autorizzati e utilizzate secondo le modalità consentite;
- **INTEGRITÀ**: le informazioni devono essere accurate, complete e modificabili esclusivamente dai soggetti autorizzati;
- **DISPONIBILITÀ**: le informazioni, i sistemi e i servizi devono essere accessibili e utilizzabili quando richiesto dagli utenti e dai processi autorizzati;
- **AUTENTICITÀ**: deve essere garantita l'identificazione certa dei soggetti, dei sistemi e delle informazioni, assicurandone la provenienza e l'affidabilità.

Il perseguimento di tali obiettivi contribuisce alla tutela del patrimonio informativo dell'Ente, alla conformità normativa, alla continuità operativa e al rafforzamento della resilienza organizzativa e digitale del Comune di Parma. L'Ente promuove pertanto l'adozione di misure adeguate a garantire la sicurezza, la continuità e la resilienza dei servizi e delle infrastrutture digitali, in coerenza con i rischi individuati e con gli obblighi normativi applicabili.

10. FRAMEWORK DOCUMENTALE

La gestione della sicurezza delle informazioni del Comune di Parma è supportata da un sistema strutturato di informazioni documentate, composto dalla documentazione organizzativa e operativa propria dell'Ente e dalla documentazione del SGSI di IT.CITY S.p.A.

Il framework documentale si articola pertanto nei seguenti livelli coordinati:

- documentazione del SGSI di IT.CITY S.p.A., applicabile alle attività affidate alla società;
- documentazione specifica del Comune di Parma, mediante la quale sono definiti il modello organizzativo, le responsabilità, le decisioni e i processi propri dell'Ente.

10.1 Framework documentale SGSI di IT.CITY S.p.A.

Il framework documentale del SGSI di IT.CITY S.p.A. costituisce il riferimento operativo e metodologico per la gestione della sicurezza delle informazioni e della cybersicurezza nell'ambito dei servizi e delle attività affidati alla società. Esso comprende le politiche, le procedure, gli standard e le ulteriori informazioni documentate del SGSI applicabili al perimetro del Comune di Parma.

Documentazione di riferimento:

- INF-SGSI-000 – Elenco documenti SGSI (disponibile nel repository documentale – sharepoint).

10.2 Framework documentale specifico del Comune di Parma

Il Comune di Parma adotta e mantiene una propria documentazione, finalizzata a definire il modello di governo della sicurezza delle informazioni e a declinare, nel contesto istituzionale e organizzativo dell'Ente, i requisiti normativi, le responsabilità, i processi e le misure applicabili. Tale documentazione è coordinata, con le politiche, le procedure e le metodologie del SGSI di IT.CITY S.p.A

Tale documentazione comprende, tra l'altro:

- Procedura per la gestione degli incidenti di sicurezza delle informazioni
- Organizzazione per la Sicurezza Informatica - Ruoli e responsabilità per la gestione della sicurezza delle informazioni
- Regolamento per l'utilizzo dei sistemi informativi e delle risorse informatiche, telematiche e telefoniche
- Macrostruttura organizzativa
- Piano di Gestione delle Vulnerabilità
- Valutazione del rischio
- Piano di Trattamento del rischio
- Piano di continuità operativa;
- Piano di disaster recovery;
- Piano di adeguamento
- Piano di gestione delle crisi
- Piano di formazione
- Sicurezza informatica dei soggetti esterni
- Politica di controllo degli accessi
- Gestione account
- Gestione della sicurezza fisica
- Audit e monitoraggio dei fornitori
- Clausole di sicurezza per fornitori e partner

I documenti comunali sopra elencati costituiscono le informazioni documentate del modello organizzativo del Comune di Parma per la sicurezza delle informazioni e sono sottoposti ad approvazione, diffusione, revisione e aggiornamento secondo le competenze definite dall'Ente. Tali documenti richiamano e integrano le informazioni documentate del SGSI di IT.CITY S.p.A. applicabili al perimetro comunale.
La presente Politica è sottoposta a riesame periodico e, comunque, in occasione di modifiche normative, organizzative, contrattuali o tecnologiche, variazioni rilevanti del perimetro, incidenti significativi o cambiamenti dell'esposizione al rischio. Il riesame tiene conto degli esiti delle attività di monitoraggio, degli audit, degli incidenti.