Comune di Parma

# PIANO DI TRATTAMENTO DEL RISCHIO

*Documento per approvazione formale ai fini ID.RA-06*

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: 15/01/2026
Ultimo aggiornamento: 24/09/2026
Codice:
Versione: 1.2
Stato:
Classificazione INTERNO

## 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) |
| 24/09/2026 | Settore Sviluppo Economico e Transizione Digitale | 1.2 | Nuova Valutazione |
| | | | |
| | | | |
| | | | |
| | | | |

## Approvazioni

| Nome | Funzione | Data | Firma |
|---|---|---|---|
| Ferioli Nicola | Dirigente Settore Sviluppo Economico e Transizione Digitale | 24/09/2026 | |
| | | | |
| | | | |

## Lista distribuzione

| |
|---|
| L'elenco delle risorse che accedono al documento è gestito e visibile sulla cartella che lo contiene su SharePoint on-line/Intranet |

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. **PIANO AZIONI DI TRATTAMENTO DEL RISCHIO** ..... 7

## 1. INTRODUZIONE

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.

Il presente Piano di Trattamento del Rischio costituisce lo strumento attraverso il quale l'Amministrazione definisce e pianifica le azioni necessarie per la gestione dei rischi relativi alla sicurezza delle informazioni individuati e valutati nell'ambito del processo di gestione del rischio.

Il Piano traduce gli esiti della valutazione dei rischi in specifiche azioni di trattamento, finalizzate a ricondurre i rischi entro livelli ritenuti accettabili dall'Amministrazione, attraverso l'individuazione delle misure da adottare, delle responsabilità, delle priorità, delle tempistiche e delle modalità di attuazione e monitoraggio.

Il Piano è predisposto sulla base degli esiti della valutazione dei rischi del Comune di Parma, svolta secondo la procedura comunale di valutazione e trattamento del rischio, che assume quale riferimento metodologico, per gli aspetti applicabili, la Procedura PR-SGSI-001 adottata nell'ambito del SGSI di IT.CITY S.p.A.

Il Piano è soggetto a periodico monitoraggio, riesame e aggiornamento in relazione all'evoluzione dei rischi, allo stato di attuazione delle misure di trattamento previste, alle modifiche rilevanti del contesto organizzativo, tecnologico e normativo, nonché agli esiti delle attività di monitoraggio e valutazione del rischio.

La titolarità operativa dei controlli introdotti o rafforzati seguendo la ISO/IEC nell'edizione 2022 è assegnata e documentata: threat intelligence (A.5.7) e monitoraggio/logging (A.8.16) al presidio SOC/CSIRT; sicurezza cloud (A.5.23), prontezza ICT (A.5.30), monitoraggio fisico (A.7.4), configurazioni (A.8.9), DLP e web filtering (A.8.12 e A.8.23) alle funzioni tecnologiche competenti; cancellazione e masking (A.8.10 e A.8.11) ai proprietari dei dati e dei processi; codifica sicura (A.8.28) ai responsabili di sviluppo e ai referenti contrattuali dei fornitori.

## 2. SCOPO E CAMPO DI APPLICAZIONE

Il presente Piano di Trattamento del Rischio ha lo scopo di definire e pianificare le misure necessarie per il trattamento dei rischi per la sicurezza delle informazioni individuati nell'ambito del processo di valutazione del rischio dell'Ente.

Il Piano individua, per ciascun rischio oggetto di trattamento, la modalità di trattamento prescelta, le azioni e le misure di sicurezza da adottare, i soggetti responsabili, le priorità e le tempistiche di attuazione, al fine di ricondurre il livello di rischio entro le soglie di accettabilità definite dall'Ente.

Il documento costituisce pertanto lo strumento attraverso il quale i risultati della valutazione del rischio vengono tradotti in interventi concreti e monitorabili, assicurando la tracciabilità tra rischi identificati, decisioni di trattamento, controlli individuati, stato di attuazione e rischio residuo.

Il Piano si applica ai rischi per la sicurezza delle informazioni compresi nel perimetro del Comune di Parma e tiene conto, per i servizi e le attività affidati, delle politiche, delle procedure, delle metodologie e delle misure previste dal SGSI di IT.CITY S.p.A.

Il Piano riguarda, in particolare, i sistemi informativi, i servizi digitali, le infrastrutture tecnologiche, i dati e le informazioni, i processi organizzativi e le risorse interessate, comprese, ove applicabile, le componenti e i servizi affidati a soggetti terzi.

Le misure di trattamento possono riguardare interventi di natura organizzativa, procedurale, tecnologica e fisica, nonché azioni relative alla gestione dei fornitori, alla formazione e sensibilizzazione del personale e al miglioramento dei processi di sicurezza.

## 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"
- Framework documentale specifico Comune di Parma
- Framework documentale IT.CITY S.P.A. Sistema di Gestione della Sicurezza delle Informazioni (SGSI)

## 4. PIANO AZIONI DI TRATTAMENTO DEL RISCHIO

Le azioni di trattamento sono registrate e dettagliate nel documento “4.1_CDP_Piano delle azioni di trattamento del rischio”. Il relativo stato di attuazione è monitorato con periodicità almeno semestrale e ogniqualvolta intervengano variazioni significative dei rischi, incidenti rilevanti, vulnerabilità critiche, modifiche organizzative o tecnologiche, variazioni dei servizi e dei fornitori oppure esiti di audit e verifiche che richiedano l’aggiornamento delle misure previste.

# Piano azioni di trattamento del rischio 24/09/2026

| REV.01 | POL-SGSI-004-A1 | Redatto: Settore Sviluppo Economico e Transizione Digitale | Controllato: EQ nel Settore Sviluppo Economico e Transizione Digitale | | Approvato:Giunta Comunale | | | Data: | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Controllo | Livello rischio | Analisi | Descrizione delle Azioni di mitigazione previste | Responsabile | Risorse economiche necessarie | Altre risorse necessarie (personale, ecc) | Data conclusione azione | Attività di formazione per personale tecnico e per utilizzatori | Modalità verifica efficacia risultati | Stato dell'azione |
| 05.18.02 Diritti di accesso - Riesame | 36 | Attualmente non viene eseguito un riesame periodico dei diritti di accesso. La normativa richiede che le autorizzazioni siano verificate a intervalli regolari (o a seguito di cambiamenti significativi) per assicurare che i privilegi rimangano coerenti con le effettive necessità operative e le mansioni correnti del personale. | Critico: Definire e implementare un processo di riesame periodico (almeno semestrale) dei diritti di accesso. Documentare gli esiti e procedere alla revoca dei privilegi non necessari. | Responsabile Transizione Digitale | incluse nel contratto di servizio con It.city | N.A. | 31/03/2027 | N.A. | Report di audit | in corso |
| 05.19 Sicurezza delle informazioni nelle relazioni con i fornitori | 27 | L'organizzazione ha integrato requisiti di sicurezza e aggiornamenti normativi nei nuovi contratti di fornitura. Tuttavia, i contratti storici non includono clausole specifiche riguardanti la sicurezza delle informazioni, l'obsolescenza tecnologica e la conformità NIS2. È necessario un allineamento omogeneo di tutto il parco fornitori critici. | Miglioramento: Revisionare i contratti in essere con i fornitori critici tramite addendum sulla sicurezza (DPA) e definire un processo di monitoraggio delle loro prestazioni di sicurezza. | Responsabile Transizione Digitale | N.A. | SETTORE POLITICHE CONTRATTUALI E SUA | 31/12/2026 | N.A. | template contratto | in corso |
| 05.22.02 Monitoraggio, riesame e gestione dei cambiamenti dei servizi dei fornitori - Monitoraggio e riesame | 27 | Il monitoraggio continuo delle prestazioni di sicurezza dei fornitori è attualmente limitato alla sola componente privacy. Manca un processo strutturato di riesame tecnico e operativo dell'efficacia dei controlli di sicurezza implementati dai fornitori durante l'intero ciclo di vita del servizio. | Azione Correttiva: Definire e implementare un piano di monitoraggio tecnico (SLA di sicurezza) per i fornitori critici, includendo riesami periodici delle prestazioni e dei log di sicurezza. | Responsabile Transizione Digitale | 20.000,00 € | fornitore esterno | 31/10/2026 | N.A. | Report di audit supply chain | in corso |
| 06.02 Termini e condizioni d'impiego | 27 | I termini contrattuali includono il Codice Etico e il Codice di comportamento e fanno riferimento alle regole di sicurezza dettagliate nel Regolamento Informatico, definendo le responsabilità legali di base. Tuttavia, manca un riferimento esplicito alle responsabilità specifiche derivanti dal Sistema di Gestione della Sicurezza delle Informazioni (SGSI) e agli obblighi di conformità NIS2 all'interno delle nomine individuali degli addetti al trattamento. | Miglioramento: Aggiornare i template delle nomine e dei contratti individuali inserendo clausole specifiche sulla responsabilità dell'utente verso il SGSI e le procedure di sicurezza aziendali. | Responsabile Transizione Digitale | N.A. | Settore Risorse Umane | 31/03/2027 | N.A. | template contratto individuale | in corso |
| 06.05 Responsabilità dopo la cessazione o il cambio d'impiego | 27 | Le responsabilità e gli obblighi di sicurezza che rimangono validi dopo la cessazione del rapporto di impiego non sono formalizzati. Sebbene l'accesso logico venga revocato, manca un impegno scritto post-contrattuale sulla riservatezza delle informazioni e una pianificazione strutturata del passaggio di consegne per gli asset critici. | Azione Correttiva: Definire una procedura di "Off-boarding" che includa la firma di un impegno di riservatezza post-impiego e un verbale di restituzione degli asset e passaggio di consegne | Responsabile Transizione Digitale | N.A. | Settore Risorse Umane | 31/03/2027 | N.A. | template modulo dimissioni/quiescienza | in corso |
| 07.03 Messa in sicurezza di uffici, locali e strutture | 27 | Uffici, locali e strutture sono protetti da accessi non autorizzati e minacce ambientali. I documenti cartacei sensibili sono custoditi in armadi chiusi a chiave e l'accesso ai locali tecnici è limitato. Il dimensionamento e la segregazione degli uffici sono progettati per prevenire l'osservazione o l'ascolto non autorizzato.<br>Gli uffici delle sedi periferiche (esempio casa della musica) non sono controllati qui di potenzialemente utilizzabili i sistemi el comune | Azione Correttiva: Completare il progetto NAC per governare gli accessi dalle postazioni remote solo per asset autorizzati | Responsabile Transizione Digitale | incluse nel contratto di servizio con It.city | Presidio TLC | 31/12/2026 | N.A. | Verbale di collaudo installazione sistema NAC e Regolamento informatico dell'Ente nella parte che riguarda la gestione degli asset non digitali | in corso |
| 07.08 Disposizione delle apparecchiature e loro protezione | 27 | Le apparecchiature ICT sono disposte in modo da minimizzare i rischi derivanti da minacce ambientali e accessi non autorizzati. Il controllo integra cablaggi sicuri (07.12) e una corretta gestione della capacità e del condizionamento (07.11) all'interno dei locali tecnici. Cio' non è confermabile nelle sedi periferiche | vedi 07.03 | Responsabile Transizione Digitale | incluse nel contratto di servizio con It.city | Presidio TLC | 31/12/2026 | N.A. | Verbale di collaudo installazione sistema NAC e Regolamento informatico dell'Ente nella parte che riguarda la gestione degli asset non digitali | in corso |
| 08.08 Gestione delle vulnerabilità tecniche | 27 | it.city gestisce le vulnerabilità attraverso l'uso di SCCM, l'analisi dei bollettini vendor (Oracle) e scansioni trimestrali con Nessus Pro. Tuttavia, il processo richiede un potenziamento nell'area dello sviluppo software interno, dove è prevista l'implementazione di strumenti di analisi statica (SAST) e dinamica (DAST) per una copertura completa del ciclo di vita applicativo. Carenti anche nella fase di remediation (non si riesce a chiudere per tempo le vulnerabilità) | Miglioramento: Implementazione e integrazione di strumenti SAST/DAST nel ciclo di sviluppo (SDLC) e consolidamento del processo di remediation delle vulnerabilità applicative entro i tempi definiti dalla policy di patching. | Responsabile Transizione Digitale | incluse nel contratto di servizio con It.city | N.A. | 31/03/2027 | necessaria da completare entro il 31/03/2027 - importo stimato 5.000 € | Report di analisi SAST/DAST | in corso |
| 08.19 Installazione del software sui sistemi in esercizio | 27 | L'attuale processo di installazione del software sui sistemi operativi e negli ambienti di produzione risulta parzialmente presidiato ma non ancora pienamente formalizzato. | Azione correttiva da definire | Responsabile Transizione Digitale | incluse nel contratto di servizio con It.city | N.A. | 31/12/2026 | N.A. | istruzione operativa (SGSI) installazione, configurazione hardening sistemi | in corso |
| 08.29 Test di sicurezza in fase di sviluppo e di accettazione | 27 | Attualmente, i test di sicurezza sono prevalentemente delegati ai fornitori esterni senza standard di verifica definiti o criteri di accettazione rigorosi da parte dell'Ente. La mancanza di test di sicurezza interni sistematici (es. Vulnerability Assessment su ambienti di pre-produzione) limita la capacità di it.city di validare autonomamente la robustezza del software prima del rilascio. | Miglioramento (Priorità Alta):<br>1. Definire un set standard di test di sicurezza obbligatori per l'accettazione del software.<br>2. Richiedere ai fornitori report dettagliati dei test di sicurezza eseguiti.<br>3. Implementare test di accettazione indipendenti (Vulnerability Assessment) prima del passaggio in produzione. | Responsabile Transizione Digitale | 5.000,00 € | fornitore esterno | 31/10/2026 | N.A. | Definizione nuovo processo per il miglioramento della verifica della sicurezza dei fornitori | in corso |