Comune di Parma

ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA

RUOLI E RESPONSABILITA' PER LA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

Documento per approvazione formale ai fini GV.RR-02

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: 03/06/2026
Codice:
Versione: 1.1
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)

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 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** 5
4. **RUOLI E RESPONSABILITA'** 6
- 4.1 **Organi di amministrazione e direttivi** 6
- 4.2 **Comitato di Crisi** 7
- 4.3 **Ruoli di coordinamento** 7
- 4.4 **Ruoli operativi e specialistici** 8
- 4.5 **Altri soggetti** 9

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.

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 documento costituisce il documento di riferimento dell'organizzazione per la sicurezza informatica del Comune di Parma ai fini della misura GV.RR-02, punto 1, dell'Allegato 1 alla Determinazione ACN n. 164179 del 14 aprile 2025. Esso definisce il modello organizzativo, i ruoli, le responsabilità e le correlate autorità in materia di sicurezza informatica, ed è approvato dagli Organi di Amministrazione e Direttivi dell'Ente.

Il documento è oggetto di riesame periodico e aggiornamento in caso di variazioni organizzative, incidenti significativi o mutamenti dell'esposizione alle minacce e ai rischi, in coerenza con quanto previsto dalla misura GV.RR-02.

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"

4. RUOLI E RESPONSABILITA'

4.1 Organi di amministrazione e direttivi

Definiscono e approvano gli indirizzi strategici in materia di sicurezza delle informazioni e assicurano che siano adottati adeguati assetti organizzativi, risorse e controlli per la gestione dei rischi. Assicurano l'attuazione operativa degli indirizzi strategici, promuovono la cultura della sicurezza e garantiscono che ruoli, responsabilità e processi siano formalizzati, comunicati e applicati.

Le funzioni di coordinamento, supervisione e riesame ivi incluse quelle relative all'analisi degli incidenti di sicurezza, sono esercitate dagli Organi di Amministrazione e Direttivi del Comune di Parma, sulla base delle informazioni fornite dal Gruppo di Coordinamento e di Gestione degli Incidenti.

In particolare, gli Organi Direttivi sono informati tempestivamente in caso di incidenti significativi e procedono al riesame periodico delle informazioni relative agli incidenti e alle misure di mitigazione adottate, al fine di indirizzare le azioni di miglioramento del SGSI.

Presidio di governance NIS2 e ISO/IEC 27001:2022

Gli Organi di Amministrazione e Direttivi, nell'ambito delle rispettive competenze istituzionali e organizzative, approvano le modalità di attuazione delle misure di gestione dei rischi per la sicurezza informatica, ne sovrintendono l'implementazione e verificano l'adempimento degli obblighi applicabili.

Approvano il piano di trattamento del rischio. Il RTD assicura la tracciabilità tra rischi, controlli ISO/IEC 27001:2022, obblighi NIS2, azioni del Piano di Adeguamento ed evidenze di attuazione.

La ripartizione formale delle competenze tra Sindaco, Giunta, Direttore Generale, Responsabile per la Transizione Digitale e ulteriori soggetti dell'Ente è documentata nella tabella sottostante:

Ruolo	**Responsabilità**
Sindaco/Giunta	Definiscono e approvano gli indirizzi strategici
Direttore Generale/Segretario Generale	Funzioni di coordinamento, supervisione e riesame degli eventi di sicurezza
Responsabile per la Transizione Digitale	Presidio NIS2 - D.Lgs. 138/2024

Affidamento delle attività operative

L'affidamento delle attività operative a IT.CITY S.p.A. o ad altri fornitori non trasferisce la responsabilità di indirizzo, approvazione, supervisione e vigilanza che resta in capo al Comune. Fermo restando il riparto formale delle competenze, i componenti degli Organi di Amministrazione e Direttivi rispondono anche personalmente delle violazioni degli obblighi loro attribuiti, nei limiti e secondo il regime previsto dal D.Lgs. 138/2024 e dall'ordinamento applicabile.

Ii Organi di amministrazione e direttivi ricevono informazioni periodiche sullo stato di attuazione delle misure e sono informati tempestivamente degli incidenti significativi e delle relative notifiche. Gli

Organi competenti assicurano, secondo le rispettive attribuzioni, che le azioni correttive siano valutate, approvate, finanziate e monitorate.

Formazione

Gli Organi di amministrazione e direttivi partecipano alla formazione specifica e periodica in materia di cybersicurezza e gestione del rischio prevista dalla normativa applicabile.

Programma, frequenza, partecipazione ed evidenze sono disciplinati dal Piano di formazione dell'Ente.

4.2 Comitato di Crisi

Il comitato di Crisi è il gruppo di direzione e coordinamento attivato in presenza di incidenti di sicurezza, eventi di indisponibilità dei servizi ICT o situazioni che possano compromettere la continuità operativa dell'Ente.

Ha il compito di assumere le decisioni strategiche, coordinare le strutture coinvolte, autorizzare le comunicazioni verso l'esterno, supervisionare le attività di risposta e ripristino e garantire il ritorno alla normale operatività.

Il Comitato di Crisi è composto dalle seguenti figure di riferimento:

- Sindaco o Assessore delegato alla Transizione Digitale
- Direttore Generale / Segretario Generale
- Dirigente Responsabile per la Transizione Digitale / CIO
- Responsabile della Comunicazione Istituzionale

In funzione della tipologia di evento, il Comitato di Crisi può avvalersi delle seguenti figure di riferimento:

- Amministratore Unico/Direttore Operativo IT.CITY S.p.A.
- Data Protection Officer (DPO)
- Responsabile Protezione Civile
- Responsabili dei servizi comunali impattati

Le modalità di attivazione, funzionamento, escalation e chiusura delle situazioni di crisi sono disciplinate dal Piano di Gestione delle Crisi dell'Ente.

4.3 Ruoli di coordinamento

- **Responsabile per la Transizione Digitale (RTD)**

  Garantisce il coordinamento complessivo delle iniziative di sicurezza delle informazioni e la coerenza con gli obiettivi istituzionali del Comune. Il ruolo di Responsabile della Sicurezza delle Informazioni è attribuito al Responsabile per la Transizione Digitale (RTD), che assicura la definizione, l'attuazione, il monitoraggio e il miglioramento del Sistema di Gestione della Sicurezza delle Informazioni, operando in coerenza con gli indirizzi e sotto la supervisione degli Organi di Amministrazione e Direttivi.
  Il RTD coordina il mantenimento del Piano di trattamento del rischio, verifica la coerenza con la documentazione, raccoglie gli indicatori di efficacia dei controlli e predispone il reporting per gli Organi di Amministrazione e Direttivi.

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.

- **Dirigenti e Responsabili di struttura (Comune e IT.CITY)**

  Assicurano l'attuazione delle policy di sicurezza e la gestione dei rischi nell'ambito delle rispettive responsabilità.

4.4 Ruoli operativi e specialistici

- **Gruppo di Coordinamento e di Gestione degli Incidenti**

  È responsabile del coordinamento operativo della gestione degli incidenti di sicurezza, assicurando l'applicazione delle procedure, il coinvolgimento delle funzioni competenti e il miglioramento continuo del processo.

- **Punto di Contatto ACN o suo sostituto**

  Cura i rapporti con l'Agenzia per la Cybersicurezza Nazionale, assicurando le comunicazioni e le notifiche previste dalla normativa vigente.

  Il Punto di Contatto ACN e il sostituto verificano con cadenza almeno annuale i dati di registrazione, i recapiti, i domini e gli indirizzi IP dichiarati, coordinano le comunicazioni istituzionali con ACN e conservano le ricevute e le evidenze.

- **Referente CSIRT**

  Figura tecnica con competenze in ambito ICT e cybersecurity che cura direttamente le attività di segnalazione e interazione con il CSIRT Italia e supporta la gestione tecnica degli incidenti di sicurezza.

- **Responsabile della Protezione dei Dati (DPO)**

  Supporta l'organizzazione nella conformità al Regolamento (UE) 2016/679 e nella gestione degli eventuali data breach.

- **Funzione Comunicazione istituzionale**

  Supporta la gestione della comunicazione interna ed esterna in caso di incidente di sicurezza, assicurando coerenza, chiarezza e controllo delle informazioni diffuse, in coordinamento con il Gruppo di Coordinamento e di gestione degli Incidenti.

- **Security Operations Center (SOC)**

  Monitora i sistemi, rileva e analizza eventi e incidenti e supporta le attività di risposta e contenimento.

- **Team IT / Specialisti IT / Amministratori di sistema**

  Attuano le misure di sicurezza tecniche, gestiscono i sistemi informativi e partecipano attivamente alla prevenzione, rilevazione e gestione degli incidenti di sicurezza.

4.5Altri soggetti

- **Personale e collaboratori**
  Il personale e i collaboratori rispettano le politiche, le procedure e le istruzioni di sicurezza applicabili, partecipano alle attività formative previste e segnalano tempestivamente eventi, anomalie, vulnerabilità o sospetti incidenti di sicurezza attraverso i canali definiti dall'Ente.

- **Fornitori e terze parti**
  Sono tenuti al rispetto dei requisiti di sicurezza definiti dal Comune di Parma e da IT.CITY, in conformità agli obblighi contrattuali.

I contratti e gli accordi con fornitori e terze parti prevedono obblighi di cooperazione, disponibilità delle evidenze e notifica tempestiva a cascata di eventi e incidenti, con tempi compatibili con gli obblighi del Comune verso CSIRT Italia e ACN. I requisiti di dettaglio sono definiti nei documenti "Audit e Monitoraggio dei Fornitori" e "Sicurezza Informatica Esterni".

Il Comune di Parma assicura la disponibilità delle informazioni e delle evidenze necessarie alle attività di vigilanza e ispezione dell'ACN e tiene conto del regime di responsabilità e sanzionatorio previsto dal D.Lgs. 138/2024

Nel documento allegato si riportano i principali fornitori e subfornitori gestiti direttamente dal Comune di Parma o da IT.CITY S.p.A. per conto dell'Ente, secondo quanto previsto dal contratto di servizio e dagli altri atti di affidamento, con l'indicazione del relativo ambito di attività.

ALLEGATO 1:

TABELLA DEI PRINCIPALI FORNITORI CON RELATIVO AMBITO DI ATTIVITA'
La presente tabella è soggetta ad aggiornamenti periodici per riflettere l'evoluzione dell'ecosistema tecnologico dell'Ente. Il censimento verrà adeguato a seguito della stipula di nuovi contratti, del subentro di ulteriori soggetti o di modifiche e varianti contrattuali intercorse nella gestione del sistema informatico.

FORNITORE	SERVIZI EROGATI
ADS Automated Data Systems S.p.A.	Suite GIPSI - Gestione Personale, Sfera e Albo Online - Iter atti, Casa di Vetro (L190) - Trasparenza
Anthesi S.r.l.	Piattaforma Elixform per configurazione ed erogazione di Servizi online
Bridge 129 Safety & Security S.r.l.	Videosorveglianza
Bieffedue Elettronica	Videosorveglianza
Cts S.r.l.	Videosorveglianza - TSCAN monitoraggio traffico
Comuni-Chiamo	Gestione Segnalazioni
Dromedian S.r.l.	Sistema conferenza e votazione Consiglio Comunale
Ecoh Media S.r.l.	Strategic PA - gestione società partecipate
Euforlegal S.r.l.	Teleforum FOR - Avvocatura
Gemmlab S.r.l.	Gemello digitale
Gruppo Marche Informatica S.r.l.	SW Cimiteri, SW Contratti
I.T. Ing. Trasp S.r.l.	Sfinge - gestione incidenti
Incloud Team S.r.l.	Connet - Processo sanzionatorio in strada
Lepida S.C.P.A.	Data center, Piattaforma ASTREA per depositi giudiziari
Maggioli S.p.A.	Suite Sicr@Web per Demografici, Stato Civile e Ragioneria, Icaro per Gestione Sociali, CatView - Catasto
Municipia S.p.A.	Engramma – protocollo e gestione PEC
Mondo Edp S.r.l.	IRIS - Timbrature e presenze
Proveco S.r.l.	MC3 - Albo Pretorio
Parma Valore Comune - PVC	Gestione Riscossioni
Redturtle S.r.l.	Portale Istituzionale e Intranet
Retelit Digital Services S.p.A.	Connettività e fonia
Semenda S.r.l.	Infrastruttura GIS e sistemi cartografici, Toponomastica - gestione stradario e civici

Sistemi E Soluzioni S.r.l.	Sep@Com - Gestione Patrimonio, Bando ERP
Starch S.r.l.	Archiweb - Gestionale edilizia e urbanistica, CPortlal - Servizi online SUE
Telecom Italia	Connettività e fonia fissa/mobile