Comune di Parma

Piano di Formazione

Documento per approvazione formale ai fini PR.AT-01

Comune di Parma

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: 14/04/2025
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
Ferioli Nicola	Settore Sviluppo Economico e Transizione Digitale	29/06/2026	

Lista distribuzione

L'elenco delle risorse che accedono al documento è gestito. Il documento è accessibili 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. La presente procedura, 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. **OBIETTIVI FORMATIVI** 6
5. **DESTINATARI E FABBISOGNI FORMATIVI** 7
6. **PIANO ANNUALE DELLE ATTIVITA' FORMATIVE** 8
7. **MODALITA' DI EROGAZIONE** 9
8. **VERIFICA DELL'APPRENDIMENTO** 10
9. **MONITORAGGIO DELL'EFFICACIA** 10
10. **APPROVAZIONE FORMALE DEL PIANO** 10
11. **REGISTRO DELLA FORMAZIONE** 11
12. **RIESAME E AGGIORNAMENTO** 11

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 Piano applica il ciclo delle clausole 4-10 della ISO/IEC 27001:2022: contesto e parti interessate, leadership, pianificazione basata sul rischio, competenze e consapevolezza, attuazione delle attività formative, valutazione delle prestazioni e miglioramento. I fabbisogni sono determinati anche mediante valutazioni del rischio, audit, incidenti, esercitazioni e Piano di Trattamento/Adeguamento.

2. SCOPO E CAMPO DI APPLICAZIONE

Il presente Piano definisce la programmazione delle attività di formazione e sensibilizzazione in materia di sicurezza delle informazioni e cybersicurezza per il personale e per i soggetti che operano per conto del Comune di Parma.

Il Piano è finalizzato a sviluppare competenze, consapevolezza e comportamenti coerenti con modello organizzativo e di governo per la gestione della sicurezza delle informazioni e della cybersicurezza ,con il D.Lgs. 138/2024 e con le misure di sicurezza applicabili.
Il documento costituisce evidenza documentata ai fini della misura PR.AT-01 e, in particolare, del punto 2 relativo all'approvazione del Piano di formazione da parte degli Organi di Amministrazione e Direttivi.
In applicazione dell'art. 23 del D.Lgs. 138/2024, i componenti degli Organi di Amministrazione e Direttivi sono tenuti a seguire una formazione specifica in materia di sicurezza informatica e promuovono l'offerta periodica di formazione al personale. La partecipazione, il completamento e gli esiti sono documentati.

Il Piano si applica alle attività formative e di sensibilizzazione rivolte ai soggetti coinvolti, a vario titolo, nel trattamento delle informazioni, nell'utilizzo dei sistemi informativi e nella gestione della sicurezza dell'Ente.

Rientrano nel campo di applicazione: Organi di Amministrazione e Direttivi, dirigenti e responsabili di struttura, personale dipendente, personale ICT, amministratori di sistema, , Punto di Contatto NIS e sostituto, Referente CSIRT, collaboratori.

Il Piano si applica inoltre, secondo criteri di proporzionalità rispetto al ruolo, alle attività svolte e ai rischi associati, ai fornitori, consulenti, tirocinanti, personale temporaneo e agli altri soggetti esterni autorizzati ad accedere alle informazioni, ai sistemi o ai servizi dell'Ente. Per tali soggetti sono definiti, ove applicabili, specifici obblighi di informazione, formazione e sensibilizzazione, nonché gli obblighi di sicurezza previsti dai relativi contratti o incarichi.

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
- 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 n. 379907/2025, recante le specifiche di base per gli obblighi di cui agli artt. 23, 24 e 25 del D.Lgs. 138/2024, che integra e sostituisce la Determinazione n. 164179/2025, con i relativi Allegati applicabili ai soggetti importanti ed essenziali e successive modifiche.
- Provvedimenti ACN vigenti in materia di Portale ACN, Punto di Contatto, Referente CSIRT, sostituti e adempimenti dei soggetti NIS.
- Framework documentale specifico Comune di Parma
- Framework documentale IT.CITY S.P.A. Sistema di Gestione della Sicurezza delle Informazioni (SGSI)

4. OBIETTIVI FORMATIVI

- Incrementare la consapevolezza del personale sui principali rischi di sicurezza informatica e sulle responsabilità individuali nella protezione delle informazioni.
- Ridurre la probabilità di incidenti derivanti da errore umano, uso improprio degli strumenti informatici o mancata osservanza delle politiche e procedure applicabili.
- Favorire la corretta applicazione delle misure organizzative e tecniche
- Promuovere la tempestiva segnalazione di eventi, anomalie, vulnerabilità e incidenti di sicurezza.
- Assicurare che i soggetti con ruoli specifici in ambito cybersecurity dispongano di conoscenze adeguate allo svolgimento dei relativi compiti.
- Supportare la conformità agli obblighi normativi applicabili, inclusi NIS2, GDPR e le misure adottate dall'ACN.
- Assicurare che i soggetti interessati conoscano le modalità di riconoscimento, segnalazione ed escalation degli eventi e degli incidenti di sicurezza, nonché, in funzione del ruolo ricoperto, il processo previsto per la qualificazione e la gestione degli incidenti significativi e per l'adempimento degli obblighi di notifica previsti dalla

normativa vigente e dalla Procedura di Gestione degli Incidenti di Sicurezza delle Informazioni.

- Sviluppare, in funzione dei ruoli e delle responsabilità assegnate, competenze coerenti con i controlli di sicurezza delle informazioni applicabili e con le misure organizzative e tecniche adottate dall'Ente, con particolare riferimento alla gestione del rischio, sicurezza dei servizi cloud, gestione delle vulnerabilità, configurazione sicura, monitoraggio, logging, protezione delle informazioni, continuità operativa, sicurezza dello sviluppo e gestione degli incidenti.

5. DESTINATARI E FABBISOGNI FORMATIVI

Destinatari	Fabbisogno formativo principale	Livello
Organi di Amministrazione e Direttivi	Responsabilità nella governance della sicurezza, NIS2, gestione del rischio, gestione crisi e decisioni strategiche.	Direzionale
Dirigenti e Responsabili di struttura	Ruoli e responsabilità, gestione del rischio, segnalazione incidenti, continuità operativa, corretta applicazione delle policy.	Gestionale
Tutto il personale	Cyber hygiene, phishing, password e MFA, uso corretto delle risorse ICT, protezione dei dati, segnalazione di eventi sospetti.	Base
Personale ICT e amministratori di sistema	Gestione vulnerabilità, logging, hardening, risposta agli incidenti, evidenze tecniche e procedure di ripristino.	Specialistico
Punto di Contatto NIS, sostituto e Referente CSIRT	Notifiche ACN/CSIRT, incidenti significativi, comunicazioni con autorità competenti e gestione dei flussi informativi.	Specialistico
Contratti, sviluppo e gestione applicativa	Sicurezza della catena di fornitura, servizi cloud, requisiti di acquisizione e manutenzione sicura, secure coding, gestione delle vulnerabilità e clausole di notifica a cascata.	Specialistico
Fornitori, consulenti e personale esterno autorizzato	Regole di accesso e utilizzo, protezione delle informazioni, obblighi contrattuali, segnalazione immediata di eventi e incidenti, continuità e restituzione/cancellazione sicura dei dati.	Proporzionato al rischio

6. PIANO ANNUALE DELLE ATTIVITA' FORMATIVE

Area formativa	Destinatari	Contenuti minimi	Modalità	Frequenza
Awareness generale	Tutto il personale	Principi di sicurezza, phishing, password, MFA, uso corretto strumenti, protezione dati e segnalazioni.	E-learning / webinar / campagne di sensibilizzazione	Annuale
Governance e NIS2	Organi Direttivi e dirigenti	Responsabilità e supervisione degli Organi di Amministrazione e Direttivi, art. 23 D.Lgs. 138/2024, gestione del rischio, registrazione e aggiornamento ACN, misure di base, reporting sugli incidenti, poteri di vigilanza e richiamo sintetico al regime sanzionatorio.	E-learning / webinar / Sessione dedicata	All'assunzione dell'incarico e successivamente secondo la periodicità definita dall'Ente, nonché in occasione di aggiornamenti normativi o organizzativi rilevanti.
Gestione incidenti	Gruppo di Coordinamento, IT, RTD, DPO, Comunicazione	Fasi della procedura, classificazione, criteri di incidente significativo, momento di conoscenza, pre-notifica 24 ore, notifica 72 ore, relazione finale entro un mese, Portale ACN, GDPR, escalation, comunicazioni ed evidenze.	Sessione dedicata ed esercitazione tabletop	Almeno annuale e dopo variazioni rilevanti o lezioni apprese
Formazione specialistica ICT	Personale ICT e amministratori di sistema	Threat intelligence, vulnerabilità e patching, sicurezza cloud, configurazioni e hardening, cancellazione e mascheramento, DLP, logging/SIEM e monitoraggio, web filtering, backup e ripristino, gestione delle evidenze e secure coding ove applicabile.	Corso specialistico	Annuale o su necessità

Area formativa	Destinatari	Contenuti minimi	Modalità	Frequenza
Nuovi assunti	Personale neoassunto	Sicurezza informatica, uso corretto risorse, phishing, segnalazione anomalie, protezione dati.	E-learning / webinar	All'ingresso
Sviluppo, acquisizione e servizi cloud	Responsabili applicativi, procurement, tecnici e fornitori software	Security by design, requisiti contrattuali, responsabilità condivise cloud, secure coding, test di sicurezza, gestione componenti e dipendenze, vulnerabilità e cancellazione/restituzione dei dati.	Corso specialistico / workshop	Annuale e prima di progetti o affidamenti rilevanti
Fornitori ed esterni	Fornitori, consulenti e personale esterno autorizzato	Regole di sicurezza applicabili, accessi, riservatezza, MFA, uso dei canali protetti, incident notification a cascata, continuità, protezione e cancellazione delle informazioni.	Briefing / e-learning / clausola formativa	Prima dell'accesso e aggiornamento periodico in base al rischio
Esercitazioni integrate	Gruppo incidenti, RTD, Referente CSIRT, DPO, Comunicazione, responsabili di servizio e fornitori critici	Simulazione di incidente significativo, indisponibilità dei canali ordinari, attivazione crisi/BC/DR, decisione sulle notifiche e comunicazioni ai destinatari.	Tabletop / simulazione tecnica	Almeno annuale e dopo cambiamenti rilevanti

7. MODALITA' DI EROGAZIONE

Le attività formative possono essere erogate mediante corsi e-learning, sessioni in aula, webinar, campagne di sensibilizzazione, simulazioni phishing e comunicazioni periodiche di awareness.

Per i nuovi assunti o per il personale che assume nuovi incarichi, è prevista una formazione iniziale coerente con il ruolo ricoperto e con il livello di esposizione ai rischi informatici.
Per i soggetti con ruoli tecnici, di coordinamento o di interlocuzione con autorità competenti, possono essere previste sessioni specialistiche e/o aggiornamenti mirati.
La formazione iniziale è erogata tempestivamente. Sono previsti aggiornamenti in caso di cambio ruolo, nuove tecnologie, mutamenti del rischio, nuovi obblighi ACN, incidenti o esiti di audit.

Le esercitazioni possono prevedere scenari caratterizzati dall'indisponibilità dei canali ordinari e, ove pertinente rispetto allo scenario considerato, il coinvolgimento dei fornitori rilevanti o critici.

8. VERIFICA DELL'APPRENDIMENTO

Al termine delle attività formative possono essere previste modalità di verifica dell'acquisizione dei contenuti, quali quiz online, questionari di apprendimento, test finali, esercitazioni pratiche, simulazioni phishing, ecc.

Gli esiti delle verifiche sono registrati, ove previste, nel Registro della Formazione e possono essere utilizzati per individuare ulteriori fabbisogni formativi o azioni di miglioramento.
In caso di mancata partecipazione, mancato completamento o esito non adeguato della verifica, possono essere previste azioni di richiamo, recupero o formazione integrativa.
Per le attività formative individuate come obbligatorie sono definiti, ove applicabili, criteri di completamento e di superamento, modalità e tempi di recupero. Il mancato completamento o l'esito non adeguato sono registrati e determinano l'attivazione delle opportune azioni di recupero, formazione integrativa o sensibilizzazione, secondo le modalità definite dall'Ente.

9. MONITORAGGIO DELL'EFFICACIA

L'efficacia delle attività formative è monitorata attraverso indicatori quali: percentuale di completamento dei corsi, risultati dei test, partecipazione alle attività, esiti delle simulazioni phishing, numero e qualità delle segnalazioni di eventi sospetti, andamento degli incidenti riconducibili a comportamenti degli utenti e risultati di audit o riesami.

Gli esiti del monitoraggio costituiscono elemento di ingresso per il riesame e per l'aggiornamento del presente Piano.
Il monitoraggio non si limita alla partecipazione, ma valuta il cambiamento dei comportamenti e l'efficacia mediante KPI e target approvati, quali tasso di completamento, punteggi, recidiva, tempi di segnalazione, risultati delle simulazioni, incidenti riconducibili al fattore umano e capacità dei soggetti con specifiche responsabilità nella gestione degli incidenti di applicare correttamente le procedure di escalation, comunicazione e notifica di propria competenza.
. Gli scostamenti aggiornano la valutazione del rischio e il Piano di Trattamento/Piano di Adeguamento.

10. APPROVAZIONE FORMALE DEL PIANO

Il presente Piano di Formazione e Sensibilizzazione per la Sicurezza delle Informazioni è approvato dagli Organi di Amministrazione e Direttivi del Comune di Parma, nell'ambito delle rispettive competenze. L'approvazione assicura la coerenza del Piano con gli obiettivi dell'Ente, con modello organizzativo e di governo per la gestione della sicurezza delle informazioni e della cybersicurezza e con gli obblighi normativi applicabili. Gli Organi di Amministrazione e Direttivi promuovono l'attuazione del Piano, assicurano il necessario indirizzo e verificano periodicamente l'adeguatezza delle attività formative rispetto all'evoluzione del contesto normativo, organizzativo, tecnologico e di rischio.

Gli Organi di Amministrazione e Direttivi ricevono almeno annualmente, e tempestivamente in caso di criticità, una relazione su attuazione, partecipazione, efficacia, mancati

completamenti, fabbisogni e risorse necessarie. La relazione supporta la supervisione prevista dall'art. 23 del D.Lgs. 138/2024.

11. REGISTRO DELLA FORMAZIONE

È mantenuto un registro aggiornato delle attività formative erogate, dei dipendenti e degli altri soggetti formati, dei contenuti trattati e delle eventuali verifiche svolte. Il Registro della Formazione costituisce evidenza dell'attuazione del Piano e viene conservato secondo le direttive interne dell'Ente.

Il Registro riporta almeno destinatario, ruolo, contenuto, data, durata, modalità, docente o fornitore, esito della verifica, eventuale recupero, attestazione e versione del materiale. Accessi e conservazione sono disciplinati nel rispetto della protezione dei dati e del sistema documentale; il periodo di conservazione è definito dall'Ente.

12. RIESAME E AGGIORNAMENTO

Il presente Piano è riesaminato almeno annualmente e, se necessario, aggiornato in caso di modifiche normative, variazioni organizzative, mutamenti del contesto di rischio, incidenti significativi, esiti di audit o lezioni apprese.

Il riesame considera inoltre cambiamenti delle determinazioni e linee guida ACN, evoluzione delle minacce, nuovi servizi cloud o fornitori, risultati del risk assessment, scostamenti dai KPI, esiti delle esercitazioni e richieste degli Organi di Amministrazione e Direttivi.

Le versioni aggiornate del Piano sono sottoposte ad approvazione secondo il processo previsto dall'Ente e rese disponibili alle articolazioni competenti.