❑ DOCUMENTO PUBBLICO	■ AD USO INTERNO	❑ RISERVATO

COMUNE DI NAPOLI

Policy di Gestione Eventi e Incidenti

Security Event and Incident Management Policy

❑ DOCUMENTO PUBBLICO	■ AD USO INTERNO	❑ RISERVATO

COMUNE DI NAPOLI

Emissione del Documento

	Nome	Ruolo
Redazione	Ciro Petrillo	Funzionario “Staff al Responsabile della Transizione Digitale e Cybersecurity a livello di Ente”
Verifica organizzativa	Francesco Essolito	EQ “Staff al Responsabile della Transizione Digitale e Cybersecurity a livello di Ente”
Approvazione	Lucio Abbate	Referente per la Sicurezza Informatica dell’Ente

Elenco delle modifiche del documento

Versione	Data	Autore	Dettagli
1.0	30/12/2025	Area Digitalizzazione e Sistemi Informativi	Prima versione del documento

❑ DOCUMENTO PUBBLICO	■ AD USO INTERNO	❑ RISERVATO

COMUNE DI NAPOLI

INDICE

❑ DOCUMENTO PUBBLICO	■ AD USO INTERNO	❑ RISERVATO

1. Introduzione

1.1 Scopo del documento

La presente Policy ha lo scopo di fornire a tutto il personale del Comune di Napoli una guida chiara e accessibile su cosa fare in caso di incidente di sicurezza o sospetto tale, al fine di garantire una risposta tempestiva, contenere eventuali danni, tutelare i dati personali e assicurare la continuità dei servizi essenziali. Ogni dipendente, collaboratore o operatore è chiamato a collaborare attivamente: la segnalazione di un incidente non è facoltativa ma un obbligo previsto dalla normativa vigente, in particolare dal Regolamento (UE) 2016/679 (GDPR), dalla Direttiva (UE) 2022/2555 (NIS2) e dalla Legge 90/2024. Tali norme impongono tempistiche stringenti per la notifica degli incidenti, e ogni ritardo può generare impatti significativi sull'Ente, sia in termini di sicurezza che di responsabilità legale. La collaborazione tempestiva e consapevole di tutto il personale è quindi essenziale per garantire la sicurezza dell'intera struttura.

1.2 Campo di Applicazione

Questa Policy si applica a tutto il personale, a qualsiasi titolo operante a favore del Comune di Napoli (dipendenti, collaboratori, consulenti, tirocinanti, personale esterno, ecc..), che, nello svolgimento delle proprie mansioni, interagisce con dati personali, sistemi informativi o servizi digitali rilevanti.

1.3 Riferimenti Normativi

- Regolamento UE 2016/679 GDPR;
- Direttiva (UE) 2022/2555 NIS2;
- Decreto legislativo 4 settembre 2024, n. 138;
- Determina dell'Agenzia per la Cybersicurezza Nazionale (ACN) n. 164179 del 14 aprile 2024, allegati 2 e 4;
- Legge 28 giugno 2024, n. 90;

1.4 Termini, Acronimi, Definizioni

Termini/Acronimi	Definizioni
ACN – Agenzia per la Cybersicurezza Nazionale	Autorità nazionale competente in materia di cybersicurezza. È responsabile, tra le altre cose, della ricezione e gestione delle notifiche di incidenti significativi ai sensi della Direttiva NIS2.
Evento di Sicurezza	Una situazione identificata di violazione delle politiche di sicurezza delle informazioni su un sistema, un servizio, una rete, o una situazione non nota precedentemente che potrebbe essere rilevante ai fini della sicurezza informatica.
Incidente di Sicurezza	Un qualsiasi evento negativo relativo alla sicurezza fisica o logica, di natura casuale,

	colposa o dolosa, che potrebbe avere una significativa probabilità di compromettere la riservatezza, integrità e disponibilità delle informazioni e/o dei relativi sistemi informativi (sistemi, applicazioni, reti ecc.).
Cyber Incident Responder/Coordinator	Figura interna del Comune di Napoli che si occupa della gestione e coordinamento degli incidenti di sicurezza.
Dati personali	Qualsiasi informazione riguardante una persona fisica identificata o identificabile, come nome, codice fiscale, dati sanitari, ecc. Ai sensi del GDPR, i dati sanitari sono considerati “categorie particolari” e richiedono tutele rafforzate.
Antivirus	Programma che protegge i computer rilevando e bloccando virus e altri software dannosi prima che possano causare danni o rubare dati.
Firewall	Sistema di sicurezza che controlla le connessioni tra il computer e Internet, bloccando gli accessi non autorizzati e proteggendo i dati sensibili.
IDS (Intrusion Detection System)	Sistema che monitora la rete o i computer per individuare tentativi sospetti di accesso o attacchi informatici.
Attacco Ransomware	Tipologia di attacco informatico che blocca l’accesso ai dati o ai sistemi, solitamente mediante cifratura, accompagnato da una richiesta di riscatto.
Malware	Termine generico per indicare qualsiasi software dannoso (come virus, trojan, ransomware) progettato per danneggiare, spiare o rubare informazioni da un computer.
Esfiltrazione di dati	Furto o trasferimento non autorizzato di dati sensibili da un sistema informatico verso l’esterno, spesso a seguito di un attacco informatico.
Violazione dei dati personali (data breach)	Qualsiasi evento che comporta la perdita, l’accesso non autorizzato, la divulgazione o l’alterazione dei dati personali trattati da un’organizzazione.

❑ DOCUMENTO PUBBLICO	■ AD USO INTERNO	❑ RISERVATO

2. Ruoli e Responsabilità

La gestione efficace degli incidenti di sicurezza richiede la partecipazione attiva e consapevole di tutto il personale. Ogni figura ha un ruolo specifico nella prevenzione, rilevazione e segnalazione degli eventi che possono compromettere dati personali, sistemi informativi o la continuità dei servizi. Di seguito sono descritti i ruoli e le responsabilità per il processo di gestione degli incidenti e degli eventi di sicurezza:

- **Soggetti interni al Comune di Napoli**

I soggetti interni al Comune di Napoli sono tenuti a prestare la massima attenzione a qualsiasi segnale o evento anomalo, quali rilevamento di accessi non autorizzati, comportamenti anomali dei sistemi informatici, tentativi di phishing via e-mail, malfunzionamenti o altre irregolarità operative. In particolare:

  - Segnalano tempestivamente ogni sospetto incidente di sicurezza o violazione dei dati al Cyber Incident Responder/Coordinator (cfr. paragrafo 4);
  - Raccolgono informazioni relative all'incidente, senza intervenire per la risoluzione dello stesso in maniera autonoma;
  - Mantengono la riservatezza su quanto osservato o segnalato, evitando qualsiasi divulgazione non autorizzata di informazioni relative all'incidente o agli eventi correlati.

- **Soggetti esterni al Comune di Napoli**

I soggetti esterni che collaborano con il Comune di Napoli, in particolare quelli incaricati della gestione tecnica dei sistemi informatici, della manutenzione delle infrastrutture digitali, dell'erogazione di servizi applicativi o del supporto operativo, sono tenuti a osservare comportamenti diligenti e conformi alle politiche di sicurezza dell'Ente. In particolare:

  - Segnalano tempestivamente al Cyber Incident Responder/Coordinator del Comune di Napoli o al referente designato qualsiasi anomalia rilevata durante le attività di gestione, monitoraggio o manutenzione, come accessi non autorizzati, malfunzionamenti, comportamenti sospetti dei sistemi o tentativi di compromissione (cfr. paragrafo 4);
  - Documentano l'evento raccogliendo log, evidenze tecniche e informazioni utili, evitando di intervenire autonomamente sulla risoluzione dell'incidente se non espressamente autorizzati;
  - Mantengono la riservatezza su quanto osservato o gestito, astenendosi dalla divulgazione non autorizzata di dati, vulnerabilità, o dettagli tecnici relativi all'incidente o ai sistemi coinvolti;
  - Collaborano attivamente con il personale interno del Comune di Napoli e/o delle Autorità nella fase di analisi, contenimento e ripristino, secondo le procedure previste dal piano di gestione degli incidenti e dalle normative vigenti.

- **Cyber Incident Responder/Coordinator**

È il soggetto incaricato di ricevere le segnalazioni di incidenti e di coordinare il processo di analisi, classificazione e gestione dell'evento. In particolare:

  - Riceve le segnalazioni da parte del personale del Comune di Napoli;

- Garantisce che le attività di risposta siano svolte in modo efficace e rapido;
- Coordina tutte le fasi tecniche: analisi, contenimento, rimozione e ripristino dei sistemi colpiti;
- Analizza gli incidenti una volta risolti, al fine di migliorare continuamente il processo di gestione;
- Monitora l'avanzamento delle azioni correttive e preventive (remediation);
- Comunica la risoluzione dell'incidente di sicurezza alle articolazioni competenti della risoluzione dell'incidente stesso.

Le attività svolte dal Cyber Incident Responder/Coordinator e le strutture di sicurezza di supporto operativo in merito alla gestione degli incidenti, sono disciplinate nel documento "*Procedura operativa di gestione incidenti*".

3. Fonti Normative

3.1 NIS2 & Legge 90/2024

La Direttiva (UE) 2022/2555, nota come Direttiva NIS2, e la Legge 28 giugno 2024, n. 90, nota come "Legge sulla Cybersicurezza", hanno introdotto obblighi di sicurezza più stringenti per gli enti che operano in settori considerati importanti.
In Italia, la Direttiva è stata recepita con il Decreto Legislativo 4 settembre 2024, n. 138 entrato in vigore il 16 ottobre dello stesso anno. Nel quadro di applicazione della normativa, il Comune di Napoli è stato individuato dall'Autorità competente come "Soggetto Importante".
Tale classificazione comporta degli obblighi specifici, tra cui quelli relativi alla gestione e alla notifica degli incidenti di sicurezza informatica. In base a quanto previsto dal decreto di recepimento della Direttiva NIS 2, ovvero il D.Lgs 138/2024, è necessaria la notifica tempestiva all'Autorità competente di ogni incidente considerato significativo.

Un incidente è considerato significativo se "*ha causato o è in grado di causare una significativa interruzione dei servizi o una perdita finanziaria rilevante per l'entità interessata, oppure che ha interessato o è in grado di interessare altre persone fisiche o giuridiche, causando danni materiali o immateriali considerevoli*" (Direttiva UE 2022/2555), ed è quindi soggetto a notifica obbligatoria all'Agenzia per la Cybersicurezza Nazionale (ACN) entro i seguenti termini:

- **Preallarme** entro 24 ore dalla conoscenza dell'incidente;
- **Notifica** completa entro 72 ore;
- **Relazione finale** entro 30 giorni.

Queste scadenze sono vincolanti per l'organizzazione, che deve quindi attivarsi tempestivamente per rispettare gli obblighi normativi ed evitare sanzioni o responsabilità.

3.1.1 Tipologia di Incidenti

Per garantire una gestione efficace degli incidenti informatici, il Comune di Napoli adotta i criteri ufficiali di classificazione degli incidenti significativi, come definiti dalla normativa nazionale. Questa classificazione aiuta a riconoscere tempestivamente gli eventi che possono richiedere una notifica alle autorità competenti.
In particolare, è obbligatorio segnalare un incidente quando l'organizzazione ha evidenza di:

- **perdita di riservatezza** verso l'esterno di dati digitali di proprietà o sotto il proprio controllo, anche parziale;
- **perdita di integrità dei dati**, con impatto verso l'esterno;
- **accesso non autorizzato** o **abuso di privilegi** a dati digitali di proprietà o sotto controllo, anche parziale.

Queste situazioni possono manifestarsi attraverso diverse tipologie di incidenti, tra cui:

- **Malware o ransomware** che impediscono l'accesso a dati o sistemi critici, compromettendo l'erogazione di servizi comunali essenziali (es. anagrafe, tributi, protocollo);
- **Accessi non autorizzati** o uso improprio delle credenziali da parte di personale interno o soggetti esterni, con potenziale compromissione dell'integrità dei dati;
- **Interruzioni o gravi rallentamenti** nei servizi digitali rivolti ai cittadini, come la gestione delle pratiche online, la prenotazione di appuntamenti o l'emissione di certificati;
- **Furto, perdita o esfiltrazione di dati personali o sensibili**, inclusi quelli relativi ai residenti, dipendenti o utenti dei servizi sociali;
- **Disattivazione o compromissione dei sistemi di sicurezza informatica** (es. antivirus, firewall) a seguito di attacchi informatici mirati;
- **Danni fisici o ambientali** (es. incendi, guasti elettrici, allagamenti) che compromettono l'infrastruttura ICT comunale e la continuità operativa dei servizi.

Il riconoscimento e la corretta segnalazione di questi eventi sono fondamentali per attivare tempestivamente le procedure di risposta e per adempiere agli obblighi di notifica previsti dalla normativa vigente.
Anche in presenza di un semplice sospetto riconducibile a tali situazioni, si raccomanda di procedere con una segnalazione tempestiva attraverso i canali preposti (par. 4.1) al fine di consentire l'attivazione delle procedure interne e garantire il rispetto delle tempistiche previste per la notifica.

3.2 GDPR

Il Regolamento (UE) 2016/679 (GDPR) è la norma europea che tutela i dati personali delle persone fisiche. Si applica anche agli enti pubblici, che trattano quotidianamente dati particolari. Il GDPR richiede che vengano adottate misure tecniche e organizzative adeguate alla protezione dei dati personali da accessi non autorizzati, perdita, alterazione o divulgazione indebita, anche in caso di eventi accidentali.
Inoltre, impone di gestire in modo strutturato eventuali violazioni dei dati, valutandole con urgenza e, se necessario, notificandole all'Autorità di controllo (Garante Privacy) e agli interessati coinvolti.
In particolare, l'art. 33 del GDPR stabilisce che:

- La notifica al Garante deve avvenire entro 72 ore dalla scoperta della violazione, salvo casi eccezionali.

3.2.1 Tipologie di Incidenti

Le violazioni dei dati personali si classificano generalmente in tre categorie, a seconda del tipo di impatto che producono:

- **Perdita di riservatezza**: i dati vengono visti, copiati o divulgati da soggetti non autorizzati;
- **Perdita di integrità**: i dati vengono modificati in modo non autorizzato o risultano corrotti;
- **Perdita di disponibilità**: i dati non sono più accessibili o lo sono solo parzialmente (es. sistemi bloccati da malware).

In tutti questi casi, il personale deve segnalare immediatamente l'evento al Cyber Incident Responder/Coordinator che, con il supporto operativo delle strutture preposte, valuterà se si tratta di una violazione soggetta a notifica ai sensi dell'art. 33 del GDPR.

4. Protocollo di Gestione degli Incidenti

In presenza di un'anomalia, di un malfunzionamento sospetto o di un evento potenzialmente rischioso per i dati o per la continuità operativa dei servizi digitali, è essenziale agire con tempestività. Anche in caso di semplice dubbio, è sempre consigliabile procedere con una segnalazione.

4.1 Obbligo di Segnalazione: Casistiche

La segnalazione è necessaria, a titolo esemplificativo non esaustivo, nei seguenti casi:

- **Invio di dati personali o documenti amministrativi a destinatari errati**, ad esempio tramite e-mail o PEC;
- **Accesso non autorizzato a informazioni riservate**, come dati anagrafici, pratiche edilizie, tributarie o sociali, da parte di soggetti non abilitati;
- **Comportamenti anomali del sistema informatico**, blocchi improvvisi o malfunzionamenti che impediscono l'operatività degli uffici comunali;
- **Ricezione di messaggi e-mail sospetti**, contenenti allegati o link potenzialmente malevoli, indirizzati a caselle istituzionali o personali;
- **Smarrimento o furto di dispositivi contenenti dati sensibili**, come computer portatili, chiavette USB, smartphone di servizio o tablet utilizzati per attività comunali.

Di seguito sono elencate le azioni che il personale è tenuto ad attuare:

1. **Interrompere immediatamente l'attività in corso**, evitando di continuare ad utilizzare il sistema o applicativo coinvolto;
2. **Raccogliere le informazioni essenziali** per la segnalazione (cosa è accaduto, quando, quale sistema è coinvolto);
3. **Segnalare tempestivamente** attraverso i canali previsti (telefono, e-mail, help desk, ecc.) oppure di persona al Cyber Incident Responder/Coordinator.

❑ DOCUMENTO PUBBLICO	■ AD USO INTERNO	❑ RISERVATO

CANALI PREPOSTI

Canali	Riferimento
Telefono	omissis
E-mail	omissis
Help Desk	omissis

In nessun caso il personale è autorizzato a intervenire direttamente sul problema o ad attuare misure di ripristino autonome. La gestione tecnica dell'incidente e la risoluzione dello stesso è affidata esclusivamente alle strutture competenti.

4.2 Rilevanza della Segnalazione Tempestiva

Una segnalazione tempestiva consente:

- di limitare l'estensione del danno e contenere eventuali conseguenze su dati e servizi;
- di rispettare le tempistiche di notifica previste dalla normativa vigente;
- di proteggere cittadini, dipendenti e l'intera organizzazione.

La protezione dei dati e la continuità operativa dei servizi digitali costituiscono una responsabilità condivisa: ogni persona operante all'interno del Comune di Napoli è tenuta a collaborare attivamente nella prevenzione e nella segnalazione tempestiva degli incidenti. Il rispetto di tale dovere è essenziale per garantire un ambiente digitale sicuro e conforme alle normative vigenti.

5. Comunicazione in Caso di Incidente e Disservizi

Il Comune di Napoli si impegna a garantire una comunicazione chiara, tempestiva ed efficace, sia all'interno che all'esterno, in caso di incidenti di sicurezza informatica o gravi disservizi che possano avere un impatto significativo su persone, enti, partner o fornitori.
A tal fine, in base alla tipologia di evento, viene individuata una struttura dedicata alla gestione delle comunicazioni, incaricata di informare con prontezza tutti i soggetti coinvolti sull'accaduto e sui possibili effetti, diretti o indiretti, che ne potrebbero derivare.
In particolare, la comunicazione sarà attivata, quando ritenuto necessario, ossia qualora l'incidente possa compromettere la continuità o la qualità dei servizi offerti, oppure se richiesto dall'Autorità nei confronti di:

- **Utenti dei servizi**, qualora l'evento possa influire negativamente sulla loro fruizione;
- **Soggetti potenzialmente esposti a una minaccia informatica**, fornendo indicazioni utili per proteggersi;
- **Pubblico**, qualora ciò sia richiesto dalle autorità competenti;
- **Interessati**, qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Tale approccio mira a garantire trasparenza, tutela delle persone coinvolte e contenimento degli impatti operativi e reputazionali, rafforzando la fiducia e la resilienza dell'organizzazione.