❑ DOCUMENTO PUBBLICO	■ AD USO INTERNO	❑ RISERVATO

COMUNE DI NAPOLI

Information Security Policy

❑ DOCUMENTO PUBBLICO	■ AD USO INTERNO	❑ RISERVATO

COMUNE DI NAPOLI

Emissione del Documento

	Nome	Ruolo
Redazione	Francesco Essolito	EQ “Staff al Responsabile della Transizione Digitale e Cybersecurity a livello di Ente”
Verifica organizzativa	Lucio Abbate	Dirigente Servizio Gestione Sistemi e Reti Tecnologiche
Approvazione	Vincenzo Ferrara	Responsabile Area Digitalizzazione e Sistemi Informativi

Elenco delle modifiche del documento

Versione	Data	Autore	Dettagli
1.0	20/10/2025	Area Digitalizzazione e Sistemi Informativi	Prima versione del documento

INDICE

1. INTRODUZIONE

1.1 Obiettivo del Documento

Il presente documento definisce l'approccio del Comune di Napoli ed i criteri generali che sono adottati da tutto il personale, dai sistemi, dai processi e dalle procedure che operano al suo interno, al fine di garantire la sicurezza informatica dell'Ente.

All'interno dell'Information Security Policy vengono definiti:

- gli obiettivi di sicurezza che essa esprime;
- i requisiti di conformità a livello normativo e di adesione a standard e best practice di settore;
- i requisiti per la concreta realizzazione degli obiettivi di sicurezza.

L'Information Security Policy non sostituisce in alcun modo le policy e procedure previste dall'Ente e richiamate dal presente documento, per le quali si fa espresso rimando.

1.2 Ambito di Applicazione

Il presente documento è indirizzato a tutti i dipendenti di ogni livello nonché ai soggetti esterni al Comune di Napoli (es. fornitori, consulenti, partner) coinvolti nella fornitura di servizi, in conformità a quanto stabilito dalla legge e a quanto previsto da specifiche policy e procedure interne.

Gli ambiti di intervento, previsti all'interno del documento in oggetto, afferiscono a tutte le risorse informatiche, ovvero tutti i beni ICT dell'Ente che concorrono alla ricezione, archiviazione, elaborazione, trasmissione e fruizione delle informazioni gestite.

1.3 Principi di riferimento

Le persone coinvolte nell'ambito di applicazione della presente Information Security Policy sono tenute ad operare in conformità con le normative di legge e nel rispetto dei seguenti principi:

- **Tracciabilità**: Le persone coinvolte garantiscono, ciascuna per la parte di propria competenza, la tracciabilità delle attività e dei documenti inerenti al processo, assicurandone l'individuazione e la ricostruzione delle fonti, degli elementi informativi e dei controlli effettuati che supportano le attività.
- **Segregazione di compiti e attività:** Principio secondo il quale si prevede la segregazione di compiti e responsabilità tra unità organizzative distinte o all'interno delle stesse, al fine di evitare che attività incompatibili risultino concentrate sotto responsabilità comuni.
- **Conformità alle leggi e coerenza con il quadro normativo di riferimento generale:** La presente Information Security Policy è definita nel rispetto delle normative vigenti nonché degli standard applicabili vigenti in materia di sicurezza informatica.
- **Poteri autorizzativi:** Gli strumenti normativi assicurano specifici livelli autorizzativi o di supervisione commisurati alle caratteristiche o alla tipologia delle attività svolte.

- **Conflitto di interessi:** Le persone coinvolte nell'ambito della presente Information Security Policy agiscono nei confronti delle controparti secondo rapporti improntati ai più alti livelli dell'etica di comportamento, evitando di assumere decisioni e di svolgere attività in conflitto, anche solo potenziale, con gli interessi dell'Ente o comunque in contrasto con i propri doveri d'ufficio.
- **Approccio basato sui rischi e sui processi:** La presente Information Security Policy, ispirata ad una logica per processi, si basa su un approccio preventivo ai rischi, contribuendo all'assunzione di decisioni consapevoli, e, ove possibile, alla traduzione dei principali rischi in opportunità.
- **Comunicazione e flussi informativi:** A ogni organo e struttura dell'Ente sono rese disponibili le informazioni necessarie per adempiere alle proprie responsabilità.
- **Coerenza con gli obiettivi dell'Ente:** La presente Information Security Policy contribuisce a una conduzione delle attività amministrativo/comunali volte allo sviluppo sostenibile, alla massimizzazione del valore dell'Ente ed alla coerenza con gli obiettivi comunali.
- **Responsabilizzazione (Accountability):** Le persone coinvolte nell'ambito del presente documento, in linea con le funzioni ricoperte e al fine di conseguire i propri obiettivi, garantiscono l'adeguatezza dell'Information Security Policy per le attività di propria competenza, partecipando attivamente al loro corretto funzionamento.

2. Riferimenti normativi

Il seguente paragrafo, fermo restando il rispetto delle policy e procedure adottate internamente dall'Ente, definisce i riferimenti normativi esterni applicabili alla policy in oggetto.

2.1 Riferimenti Interni ed Esterni

- Regolamento (UE) 679/2016 (GDPR);
- D. Lgs. 196/2003 "Codice in materia di protezione dei dati personali" così come novellato dal D. Lgs. 101/2018 recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE/679/2016;
- D. Lgs. 82/2005 Codice Amministrazione Digitale – CAD così come novellato dalla L. 41/2023;
- Regolamento recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la pubblica amministrazione, le modalità di migrazione, nonché le modalità di qualificazione dei servizi cloud per la pubblica amministrazione, Determina n. 628/2021;
- Linee guida dell'European Data Protection Board ("EDPB") relative all'uso dei servizi cloud nel settore pubblico;
- Framework Nazionale per la Cybersecurity e Data Protection;
- ISO/IEC 27001:2022 Tecnologia dell'informazione – Tecniche di sicurezza – Sistemi di gestione della sicurezza delle informazioni – Requisiti;
- ISO 22301 - Sicurezza della società - Sistemi di gestione della continuità operativa – Requisiti.
- D.lg. 4 settembre 2024, n. 138 "Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148.":

- Legge 28 giugno 2024, n. 90 “Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici.”
- Determinazione ACN 164179 del 14 aprile 2025 “*Specifiche di base per l'adempimento agli obblighi di cui agli articoli 23, 24, 25, 29 e 32 del decreto NIS per i soggetti importanti*”;
- Comune di Napoli – Modello di Governance.

3. DEFINIZIONI, ABBREVIAZIONI E ACRONIMI

Termine/Abbreviazione	Definizione
ARDI	Area Digitalizzazione e Sistemi Informativi
CSP	Cloud Service Provider
Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («**interessato**»). Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Informazione	Insieme strutturato di dati che può essere gestito attraverso diversi strumenti (es. supporto cartaceo, elettronico, DB, comunicazione orale).
Principio del “minimo privilegio”	Principio di sicurezza secondo il quale ad un utente viene concesso il privilegio minimo indispensabile che consente il livello di accesso necessario a svolgere le attività lavorative di sua competenza.
Principio del “Need to Know”	Principio di sicurezza secondo il quale ciascun utente deve essere a conoscenza delle sole informazioni a lui necessarie per lo svolgimento delle sue attività lavorative.
Trattamento	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
Dipendente	Qualunque dipendente del Comune di Napoli autorizzato ed abilitato ad accedere a risorse informative o ad utilizzare servizi informatici dell’Ente.

4. GOVERNANCE DEI PROCESSI DI SICUREZZA INFORMATICA

La sezione descrive, in modo chiaro e sintetico, i ruoli e responsabilità degli attori coinvolti nel presente documento, sintetizzandone le attività chiave da svolgere al fine di garantire che gli obiettivi di sicurezza siano raggiunti all'interno dell'Ente. Per una panoramica più approfondita riguardo ai ruoli e alle responsabilità definite dal Comune di Napoli, con particolare riferimento alla gestione della sicurezza informatica, si rimanda al documento "*Comune di Napoli - Modello Organizzativo*".

Tutte le Aree del Comune di Napoli, tenuto conto dei loro compiti e delle responsabilità, contribuiscono alla sicurezza informatica dell'Ente, rispettando e facendo rispettare a tutto il personale i principi sanciti nel presente documento, secondo un approccio di Security by Design e garantendo l'integrazione dei requisiti di sicurezza nei processi dell'Ente.

Infine, l'Area Digitalizzazione e Sistemi Informativi si impegna a fornire supporto a tutte le Aree del Comune di Napoli al fine di garantire la sicurezza informatica. A tal fine, il Comune di Napoli ha designato il **Referente per la Cybersicurezza/Punto di Contatto** e il **Referente per la Cybersicurezza Vicario/Sostituto Punto di Contatto**. In particolare, nella seguente tabella vengono riportati i compiti in carico a ciascun soggetto coinvolto nei processi di sicurezza del Comune di Napoli:

Organi di Amministrazione e Direttivi	Gli Organi di Amministrazione e Direttivi promuovono la cultura della sicurezza delle informazioni, sovrintendono all'implementazione degli obblighi e sono responsabili di eventuali violazioni e non osservanza della normativa vigente in materia di cybersicurezza.
Dirigenti	I Dirigenti si impegnano a far rispettare il presente documento e i documenti che ne discenderanno, a tutti i dipendenti a loro sottoposti ed a svolgere un ruolo di indirizzo e controllo delle strategie di sicurezza informatica promosse dal Comune di Napoli.
Dipendenti	I dipendenti di ogni livello del Comune di Napoli si impegnano a contribuire alla sicurezza informatica dell'Ente rispettando le direttive della presente policy e delle successive policies che ne discenderanno, ed attuando le procedure di sicurezza applicabili.
Soggetti esterni	Tutti i fornitori esterni, Consulenti, Partner o qualsiasi soggetto autorizzato ed abilitato ad accedere a risorse informative o ad utilizzare servizi informatici del Comune di Napoli si impegnano a far rispettare il presente documento.

Referente per la Cybersicurezza (in adempimento alla Legge 90/2024) **Punto di Contatto (in adempimento al D. Lgs. n. 138/2024)**	Persona incaricata di sviluppare e implementare le politiche e le procedure di sicurezza informatica, nonché punto di contatto primario dell'Amministrazione con l'Agenzia per la Cybersicurezza Nazionale (ACN), in relazione a quanto previsto dalle normative vigenti in materia di cybersicurezza, cui è soggetto il Comune di Napoli. Approva le modalità d'implementazione delle misure di sicurezza nel rispetto delle presenti indicazioni strategiche degli Organi di Amministrazione e Direttivi
Referente per la Cybersicurezza vicario (in adempimento alla Legge 90/2024) **Sostituto Punto di Contatto (in adempimento al D. Lgs. n. 138/2024)**	Persona incaricata di affiancare ed eventualmente sostituire, in caso di assenza o impedimento, il Referente per la Cybersicurezza nello svolgimento degli incarichi ad esso assegnati nell'ambito di quanto previsto dalle normative vigenti in materia di cybersicurezza, cui è soggetto il Comune di Napoli.
Team di Sicurezza Informatica	Gruppo di esperti che supporta il Referente per la Cybersicurezza nelle attività finalizzate a proteggere i sistemi informatici, le reti e i dati dell'Ente da minacce e attacchi informatici attraverso, ad esempio, attività di monitoraggio, la risposta agli incidenti ecc.
Area Digitalizzazione e Sistemi Informativi	L'ARDI del Comune di Napoli gestisce e coordina tutte le attività legate ai sistemi informativi e alle tecnologie dell'informazione. I suoi compiti principali includono la pianificazione strategica IT, la gestione delle infrastrutture tecnologiche, la sicurezza informatica, il supporto tecnico ai dipendenti, la gestione dei progetti IT, il supporto alle attività di formazione del personale nonché l'innovazione tecnologica e la conformità alle normative vigenti in materia di sicurezza informatica.

4.1 Deroghe

Per garantire un adeguato livello di sicurezza informatica a livello di Ente, è fondamentale che tutte le Aree del Comune di Napoli operino in collaborazione con l'Area Digitalizzazione e Sistemi Informativi ed il team di sicurezza informatica, nel rispetto dei principi e dei processi di sicurezza descritti all'interno della presente Information Security Policy.
Qualora il Responsabile di un Servizio del Comune di Napoli abbia necessità di operare, nell'ambito dell'espletamento del proprio mandato, in deroga ai processi descritti nel presente documento, è tenuto a darne comunicazione formale a mezzo di Nota Protocollata al Direttore

Generale del Comune di Napoli e all'Area Digitalizzazione e Sistemi Informativi nella figura del Punto di Contatto. Quest'ultima, in coordinamento con il Responsabile richiedente ed eventuali altre figure coinvolte nel processo di sicurezza in questione, procederà ad una valutazione preliminare dei rischi associati alle attività in deroga. Tale valutazione dovrà poi essere comunicata e discussa con il Direttore Generale, al quale spetterà il compito di accettare il rischio o rendere fattive le implementazioni di mitigazione dello stesso.
In caso di mancata comunicazione o di comunicazione non tempestiva da parte dei soggetti sopra menzionati, qualora sussistano comprovate ragioni di urgenza nell'espletamento delle attività in deroga, il Responsabile del Servizio può procedere previa accettazione formale dei rischi.

5. Information Security Policy

Il Comune di Napoli, per lo svolgimento delle sue funzioni istituzionali, ricerca la massima efficienza utilizzando a supporto modelli innovativi di organizzazione e pianificazione.

Per il conseguimento dei suoi obiettivi, il Comune è impegnato nello sviluppo di azioni di adeguamento e miglioramento strutturale dei sistemi informativi, in particolare curando la loro evoluzione nel rispetto degli standard di qualità e di sicurezza e garantendo il continuo miglioramento dei sistemi impiegati per lo svolgimento delle attività e dei processi che presiedono all'erogazione dei propri servizi.

Pertanto, la sicurezza informatica assume un ruolo di primaria importanza nel garantire la protezione delle informazioni dalle minacce, il raggiungimento degli obiettivi istituzionali, la minimizzazione dei danni in caso di incidenti e la massimizzazione delle opportunità di miglioramento della postura di sicurezza dell'Ente.

Gli obiettivi perseguiti nell'ambito della presente Policy sono i seguenti:

- una gestione globale dei rischi legati alla sicurezza informatica e dei sistemi corrispondenti;
- il monitoraggio efficace ed il continuo miglioramento della sicurezza informatica;
- l'adempimento di principi regolatori e contrattuali;
- un adeguato livello di garanzia nelle relazioni con terzi;
- la riservatezza, l'integrità e la disponibilità delle informazioni;
- protezione di tutte le informazioni del patrimonio dell'Ente.

Il conseguimento di questi obiettivi viene assicurato attraverso la salvaguardia dei requisiti di sicurezza informatica legati alla Riservatezza, Integrità e Disponibilità.

5.1 Sicurezza delle Risorse Umane

Al fine di ridurre il rischio di errori umani, furti, frodi o usi impropri delle informazioni, è necessario che tutti i dipendenti, nonché i soggetti esterni eventualmente coinvolti nelle attività presso l'Ente, adottino regole per la sicurezza nella definizione dei ruoli e delle responsabilità e misure atte a minimizzare i danni causati da incidenti e malfunzionamenti.
Tali misure comprendono anche l'erogazione di attività di formazione, aggiornamento e sensibilizzazione, al fine di mantenere un adeguato livello di consapevolezza, idoneo a

garantire la sicurezza informatica ed un atteggiamento di vigilanza continua che consenta di rilevare e segnalare prontamente eventuali incidenti.

5.1.1 Norme durante il rapporto di lavoro

Il Comune di Napoli richiede ai propri dipendenti nonché ai soggetti esterni eventualmente coinvolti nelle attività presso l'Ente, di applicare i requisiti di sicurezza in accordo con quanto stabilito dalle policy e dalle procedure dell'Ente.
Tutti i dipendenti del Comune di Napoli ed il personale relativo a soggetti esterni eventualmente coinvolto nelle attività presso l'Ente, ove necessario, in base alla rilevanza della funzione lavorativa assunta, ricevono una formazione appropriata regolarmente aggiornata sulle policy e procedure organizzative.
È previsto, un processo disciplinare formale per i dipendenti che commettono violazioni di sicurezza; inoltre, per i fornitori esterni che operano per conto del Comune di Napoli, le violazioni delle norme di sicurezza e protezione dei dati possono comportare la risoluzione del contratto, nelle modalità previste dalle clausole risolutive presenti nel contratto stesso.

5.1.2 Cambiamento o cessazione del rapporto di lavoro

Tutti i dipendenti nonché i soggetti esterni eventualmente coinvolti nelle attività presso l'Ente, restituiscono gli asset in loro possesso subito dopo la conclusione del loro impiego, contratto, accordo o nei casi di cambio mansione; per asset si intendono sia quelli fisici che quelli logici (documenti) per i quali va sempre previsto un formale passaggio di consegne.
I diritti ed i privilegi relativi alle utenze di ciascun dipendente nonché alle utenze del personale di soggetti esterni eventualmente coinvolti nelle attività presso l'Ente e che accedono alle informazioni od utilizzano gli strumenti informatici del Comune di Napoli devono essere rimossi subito dopo la conclusione del loro impiego, contratto o accordo, o, in alternativa, sono rivisti a seguito di una modifica dell'impiego.

5.2 Gestione degli Asset

Al fine di garantire e mantenere un livello idoneo di sicurezza e protezione necessaria, sia per i beni strumentali che per i beni informativi di pertinenza del Comune di Napoli è necessario che tutti gli asset rilevanti siano censiti e classificati in relazione al loro valore rispetto ai parametri di "riservatezza", di "integrità" e di "disponibilità", ivi inclusi quelli acquistati o appartenenti a terze parti.

5.2.1 Sicurezza dei sistemi informatici e delle postazioni di lavoro

Gli apparati informatici devono essere adeguatamente posizionati e protetti, in modo tale da ridurre i rischi provenienti da eventi naturali o di natura dolosa.
I sistemi di elaborazione delle informazioni, al fine di garantire il regolare svolgimento delle attività e la continuità dei processi che presiedono all'erogazione dei servizi, devono essere situati in aree sicure, protette da un perimetro di sicurezza e da adeguati controlli ai varchi di ingresso delle aree in cui sono ubicati. Tali sistemi sono, inoltre, fisicamente protetti da accessi non autorizzati, danni fisici e interferenze.

Devono essere assicurate le forniture dei servizi necessari e di adeguate condizioni ambientali. In particolare, viene valutata la pericolosità dei principali eventi dannosi possibili e dei rischi associati. A seguito della valutazione del rischio, sono individuate e adottate le opportune contromisure.
Le linee dati di supporto ai servizi informativi devono essere protette per impedire danneggiamenti ed intercettazioni.
È necessario, inoltre, che gli apparati siano sottoposti ad adeguati piani di manutenzione, al fine di garantire la loro integrità e disponibilità. Tutte le informazioni contenute negli apparati o nei supporti in dismissione, o in manutenzione presso il personale competente del Comune di Napoli nonché presso fornitori esterni, devono essere preventivamente rimosse in modo sicuro.

5.2.2 Utilizzo dei Personal Computer e di altri dispositivi mobili

Al fine di prevenire e mitigare i rischi derivanti dall'utilizzo di sistemi mobili o rimovibili, si definiscono regole puntuali per una corretta gestione di tali sistemi, specie se utilizzati in ambienti non protetti o esterni alle sedi del Comune di Napoli. L'utilizzo di PC, cellulari o altre risorse elaborative presso aree esterne alle sedi del Comune di Napoli deve essere espressamente autorizzato ed avvenire nel rispetto delle regole previste dal presente documento nonché dalle procedure di sicurezza del Comune di Napoli.
Le postazioni di lavoro mobili sono utilizzate garantendo, in qualsiasi ambiente operativo, la protezione delle informazioni critiche da accessi fisici e logici non autorizzati e dalle minacce di carattere ambientale, anche di tipo accidentale, in conformità con le politiche di sicurezza previste dell'Ente.
Per maggiori infomazioni si faccia riferimento alla procedura per il corretto utilizzo dei sistemi informatici.

5.2.3 Protezione da malware

Il Comune di Napoli stabilisce una politica per l'identificazione e l'attuazione di specifici controlli che rilevino, prevengano e ripristinino i sistemi dopo attività dannose come accessi non autorizzati e malware. Inoltre, il Comune prevede l'implementazione di misure tecniche di sicurezza (es. installazione di software di protezione da malware) sui sistemi in uso presso l'Ente, garantendo un approccio flessibile e adattabile alle evoluzioni delle minacce informatiche.

5.2.4 Classificazione delle informazioni

Le informazioni costituiscono un elemento strategico del patrimonio informativo del Comune di Napoli e devono essere gestite in modo adeguato per sostenere i processi e i servizi dell'Ente. È fondamentale eseguire un censimento dei dati e designare un Owner dell'informazione, responsabile del trattamento e della conservazione.
La classificazione delle informazioni, descritta nell'apposita documentazione di dettaglio del Comune di Napoli all'interno della quale vengono elencate e definite le differenti categorie di informazione, deve garantire un livello di protezione appropriato in base alla loro importanza e criticità. A tal proposito, il processo di classificazione deve essere attuato nel rispetto delle seguenti attività:

1. **Censimento dei dati**: Identificare e registrare tutti i dati appartenenti al patrimonio informativo dell'Ente.
2. **Designazione dell'Owner**: Assegnare un responsabile per ogni serie di dati.
3. **Classificazione delle informazioni**: Etichettare le informazioni secondo i criteri delineati nelle politiche di dettaglio;
4. **Riclassificazione e declassificazione**: Rivedere periodicamente la classificazione delle informazioni in base a cambiamenti nei processi o nel contesto normativo.
5. **Monitoraggio della conservazione**: Assicurare che l'archiviazione delle informazioni sia conforme alle politiche di sicurezza dell'Ente.
6. **Applicazione di controlli di sicurezza**: Implementare misure di sicurezza adeguate in base alla classificazione delle informazioni.
7. **Cancellazione e distruzione sicura**: Garantire lo smaltimento sicuro dei documenti e dei supporti contenenti dati al termine del loro ciclo di vita.

Queste attività devono essere integrate nelle operazioni quotidiane del Comune di Napoli per garantire una gestione efficace e sicura delle informazioni.

5.3 Controllo degli accessi

Il Comune di Napoli stabilisce i criteri per la gestione dell'accesso degli utenti, al fine di garantire che i diritti di accesso ai sistemi informativi siano autorizzati, concessi e gestiti in modo idoneo. L'accesso ai dati deve essere fornito in relazione alle attività ed alle mansioni svolte dagli utenti. Al fine di rilevare attività non autorizzate, il Comune di Napoli predispone un sistema di controllo e ne stabilisce i criteri di utilizzo e di accesso. Tutti i dispositivi connessi alla rete dell'Ente devono essere preventivamente identificati e autorizzati e rispondere alle policies di sicurezza stabilite.

5.3.1 Controllo degli accessi logici

In riferimento al controllo degli accessi logici sono definite regole per la gestione delle credenziali degli utenti e per la gestione dei profili di accesso alle risorse dell'Ente. In particolare, le suddette regole disciplinano il processo di:

- Creazione delle utenze;
- Reset delle credenziali relative alle utenze esistenti;
- Modifica di utenze;
- Disabilitazione delle utenze;
- Revisione periodica delle utenze.

Tali processi, supportati da appositi strumenti, tengono conto dei seguenti principi:

a) *Least Privilege*: gli utenti devono aver accesso unicamente ai servizi per cui sono stati autorizzati, sulla base del principio "del privilegio minimo";
b) *Identificativo univoco*: ogni dipendente deve avere un unico identificativo. Eventuali eccezioni sono individuante, ad esempio, rispetto alle utenze relative agli amministratori di sistema/dominio, i quali sono dotati di un'utenza privilegiata, oltre all'utenza nominale, al fine di consentire il controllo e la gestione degli accessi alle risorse da parte di tutti gli utenti del Comune di Napoli.

5.3.2 Controllo degli accessi fisici

Al fine di prevenire interruzioni dell'attività operativa o accessi fisici non autorizzati, furti, perdite e danni alle informazioni ed ai beni, il Comune di Napoli prevede misure idonee per la protezione dei sistemi di elaborazione e di conservazione delle informazioni, in relazione alla loro criticità e rilevanza.
Inoltre, sono previsti opportuni meccanismi di protezione delle apparecchiature hardware e degli archivi informativi di proprietà del Comune di Napoli, con l'obiettivo di limitare o contenere eventi accidentali o dolosi nonché tentativi di intrusione.

5.4 Security By Design

Il principio della Security by Design interviene nella ideazione e sviluppo di ogni nuovo servizio, prodotto e componente dei sistemi informativi o di ogni aggiornamento significativo di un sistema esistente, con l'obiettivo primario di identificare, valutare e gestire i potenziali rischi di sicurezza che il servizio, prodotto e componente introduce sui sistemi IT dell'Ente.
Il principio della Security by Design è un processo integrato che prevede la definizione di regole e requisiti di sicurezza che saranno incluse nei processi di progettazione, sviluppo ed esercizio al fine di garantire una gestione organica della sicurezza, affidabile ed efficiente durante l'intero ciclo di vita di ogni sistema in uso presso il Comune di Napoli.
Le principali attività identificate e suggerite dall'approccio di Security by Design nelle varie fasi di sviluppo e gestione di un sistema e/o componente IT sono:

- Definizione dei requisiti di sicurezza;
- Valutazione di soluzioni o servizi e dei relativi fornitori;
- Valutazione dei rischi in materia di protezione delle informazioni;
- Definizione di clausole contrattuali inerenti alla sicurezza da includere nei contratti con i fornitori;
- Identificazione e attuazione dei controlli di sicurezza per il trattamento e la mitigazione del rischio;
- Contribuzione alla progettazione del sistema di sicurezza;
- Definizione ed esecuzione di piani di monitoraggio della sicurezza ed esecuzione di ict security assessment;
- Contribuzione alla formazione e awareness sulle tematiche di security.

5.4.1 Backup

Al fine di garantire il regolare svolgimento delle attività e la continuità dei processi che presiedono all'erogazione dei propri servizi, sono previste attività e procedure operative di backup. È necessario, pertanto, che i dati duplicati vengano archiviati in un luogo sicuro e protetti da adeguate misure di sicurezza sia all'interno dell'Ente sia nel caso in cui vengano archiviati presso sedi esterne allo stesso.
Il sito esterno usato per archiviare i backup deve essere localizzato ad una distanza sufficiente per assicurare la disponibilità degli stessi in caso di disastro presso una delle sedi del Comune di Napoli.

5.4.2 Logging e Monitoraggio

Il Comune di Napoli stabilisce i criteri per il monitoraggio ed il tracciamento delle attività degli utenti, nonché dei guasti e degli eventi impattanti la sicurezza informatica dell'Ente.

I registri finalizzati a documentare gli eventi nonché qualsiasi informazione inerente alla sicurezza devono essere adeguatamente protetti e controllati regolarmente da parte del personale del team di sicurezza informatica dell'Area Digitalizzazione e Sistemi Informativi.

5.5 Gestione del rischio cyber

Il Comune di Napoli stabilisce una metodologia di analisi del rischio, attraverso la quale individua i rischi, le azioni e le opportunità che devono essere affrontate per assicurare la gestione degli stessi e per far sì che l'Ente sia in grado di prevenire e ridurre potenziali e futuri eventi dannosi, raggiungendo i risultati attesi e perseguendo il miglioramento continuo.
Con l'obiettivo di proteggere i sistemi del Comune di Napoli dai rischi relativi alla sicurezza informatica e ridurre il grado di esposizione degli stessi a livelli coerenti con gli obiettivi operativi imposti dell'Ente ed in conformità con le normative vigenti, sono definite e implementate attività periodiche di assessment, finalizzate all'identificazione delle minacce informatiche, delle vulnerabilità ed all'elaborazione di specifici piani di mitigazione dei rischi legati alle stesse. Inoltre, in conformità con l'articolo 2 della Legge 90/2024, il Comune di Napoli si impegna a sanare le vulnerabilità segnalate dall'Agenzia per la Cybersicurezza Nazionale (ACN) entro 15 giorni dalla segnalazione, garantendo così un'adeguata e tempestiva protezione dei propri sistemi informatici.
Per maggiori dettagli si rimanda alle procedure di dettaglio definite dall'Ente.

5.6 Gestione degli incidenti relativi alla sicurezza informatica

Il Comune di Napoli, in conformità alle vigenti normative, standard e best practice di settore, stabilisce puntuali criteri per la gestione degli incidenti di sicurezza informatica, al fine di minimizzare il danno potenziale e ripristinare il normale funzionamento dei sistemi interessati dagli incidenti.
Ciascun dipendente del Comune di Napoli si impegna a segnalare prontamente eventuali malfunzionamenti nonché problematiche che interessino i sistemi da loro impiegati per l'espletamento delle attività lavorative, al fine di prevenire potenziali incidenti di sicurezza. Le segnalazioni devono pervenire al personale preposto alla gestione degli incidenti di sicurezza informatica, il quale procede, ove applicabile, alle opportune notifiche alle Autorità ed organi competenti.
Ai fini della corretta gestione di un evento impattante sulla sicurezza informatica dell'Ente, il Comune di Napoli attraverso apposita procedura:

- Recepisce i criteri di classificazione degli incidenti informatici;
- Definisce i flussi operativi per la gestione degli incidenti al fine di monitorare, rilevare e rispondere agli stessi;
- Rispetta le tempistiche di notifica alle Autorità e le relative modalità di comunicazione interna ed esterna;
- Indirizza le operazioni per la gestione di eventuali illeciti informatici, nonché la violazione di policy dell'ente o delle normative cogenti;
- Introduce misure organizzative e di controllo rilevanti;
- Prevede che sia svolta un'analisi post-incidente per esaminare l'accaduto e, sulla base del principio del "*Lesson Learned",* identificare le aree di miglioramento e sviluppare strategie per prevenirne il ripetersi in futuro.

5.7 Gestione della Continuità Operativa

Per garantire la continuità dei servizi, in caso di interruzioni dovute a guasti o disastri, il Comune di Napoli deve implementare un processo di gestione della continuità operativa. Questo processo si basa su una valutazione del rischio condivisa, che mira a ridurre gli impatti sulla operatività a livelli accettabili.
È necessario predisporre Piani di Continuità per i servizi e i processi critici, che definiscano chiaramente le responsabilità, le procedure e le risorse necessarie per garantire la continuità. Ogni Piano deve includere almeno le tematiche di seguito riportate:

- Le finalità e l'ambito di applicazione;
- L'identificazione delle responsabilità del personale coinvolto;
- I criteri per l'attivazione del Piano in caso di eventi dannosi;
- Le procedure di risposta e comunicazione per gestire le crisi;
- Le modalità di reperimento delle risorse per il ripristino.

I Piani devono essere coerenti tra loro e testati regolarmente per garantirne l'efficacia e il miglioramento continuo. È fondamentale eseguire test periodici per valutare l'adeguatezza dei Piani e mantenerli aggiornati in risposta a cambiamenti normativi, organizzativi, operativi o tecnologici.

5.8 Sicurezza nei processi di Change Management

Tutte le modifiche apportate ai sistemi nonché alle applicazioni, devono essere oggetto di un processo formale di Change Management, che garantisca che le modifiche siano state correttamente ideate, testate, documentate e autorizzate. Sulla base delle modifiche effettuate e delle minacce alla sicurezza osservate, è necessario che i test vengano ripetuti regolarmente al fine di comprendere i potenziali scenari di attacchi. È necessario, inoltre, che siano preventivamente testate e previste apposite procedure di *rollback* per il ripristino della situazione ex-ante in caso di problemi. Infine, è necessario definire idonee procedure e strumenti per il tracciamento delle modifiche e per la successiva verifica, soprattutto quando trattasi di modifiche effettuate in situazioni di emergenza.

5.8.1 Manutenzione dei sistemi informatici

In un'ottica di miglioramento continuo, è necessario garantire la manutenzione dei sistemi informatici impiegati per l'espletamento delle attività attraverso:

- la definizione di criteri e modalità per l'aggiornamento periodico dei prodotti utilizzati;
- la pianificazione e l'attuazione di interventi di manutenzione programmata (dismissione, sostituzione, ecc.);
- il collaudo dell'operatività dei sistemi dopo gli interventi di aggiornamento e manutenzione;
- l'aggiornamento della configurazione del sistema in funzione delle modifiche apportate all'ambiente, nonché la gestione di vulnerabilità emerse.

Tutte le attività di manutenzione, inoltre, devono essere tracciate e regolarmente verificate.

5.9 Gestione dei Servizi di Fornitura

Il Comune di Napoli identifica e documenta i requisiti di sicurezza per la mitigazione dei rischi associati all'accesso dei fornitori agli asset in uso presso l'Ente. Com'è noto, le informazioni possono essere messe a rischio dai fornitori con una gestione non adeguata della sicurezza informatica.
Mediante gli accordi stipulati con i fornitori si devono individuare apposite clausole e requisiti contrattuali in ambito cyber security da indirizzare per i rischi associati alla sicurezza informatica, insiti nei servizi informativi e comunicativi e nell'acquisizione di prodotti presso terze parti.
Più precisamente, tutti i requisiti relativi alla sicurezza informatica devono essere implementati e condivisi con tutti i fornitori che potrebbero trattare informazioni o fornire componenti dell'infrastruttura IT del Comune di Napoli.

5.9.1 Sicurezza dei servizi di Cloud Computing

Il Comune di Napoli definisce i requisiti di sicurezza per la progettazione, l'implementazione e la gestione dei servizi di Cloud Computing erogati all'Ente da parte dei fornitori esterni (Cloud Service Providers, "CSP"), alla luce del Regolamento AgID recante i livelli minimi di sicurezza per la qualificazione dei servizi cloud della pubblica amministrazione.
Tali attività, infatti, devono essere condotte con modalità idonee a garantire il raggiungimento ed il mantenimento nel tempo dei seguenti obiettivi generali di sicurezza:

- Conformità alle vigenti normative nazionali;
- Conformità alle norme settoriali, agli standard internazionali ed alle linee guida di riferimento;
- Conformità alle politiche di sicurezza previste internamente dall'ente;
- Protezione dell'operatività e dei processi essenziali erogati dal Comune di Napoli.

In particolare, devono essere definiti i requisiti di sicurezza per tutte le tipologie di Cloud Computing (SaaS, PaaS, IaaS). Tali requisiti devono, inoltre, tener conto del livello di condivisione delle risorse e delle tipologie di infrastrutture impiegate, al fine di identificare le misure di sicurezza più adeguate.

5.10 Conformità alle normative vigenti

Il Comune di Napoli stabilisce una politica volta a garantire la conformità dei propri sistemi con le vigenti normative e standard di sicurezza, attraverso regolari e periodiche attività di verifica e conformità normativa.
Durante le verifiche tecniche, devono essere previste misure di sicurezza per la salvaguardia sia del sistema o servizio oggetto di verifica, sia delle informazioni raccolte durante tale attività.
Particolare attenzione è, inoltre, riservata alla normativa prevista in materia di protezione dei dati personali ai sensi del Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 "General Data Protection Regulation", (di seguito "GDPR").
Il Comune di Napoli, si conforma a quanto disposto dal Regolamento summenzionato, al fine di garantire che i dati personali trattati nell'ambito dell'espletamento dei propri servizi siano adeguatamente protetti e tutelati.
A tal riguardo, ciascun dipendente del Comune, nello svolgimento di qualsiasi attività di trattamento dei dati personali, soprattutto se sensibili e/o giudiziari:

- Acquisisce unicamente i dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati;
- Rispetta il generale principio di liceità e trasparenza del trattamento;
- Cura l'esattezza e l'aggiornamento dei dati;
- Custodisce e controlla i dati personali oggetto di trattamento in modo che sia ridotto al minimo il rischio di divulgazione, distruzione o perdita, anche accidentale, degli stessi.

6. Revisione e aggiornamento del documento

Il presente documento è sottoposto ad approvazione formale da parte degli organi amministrativi e direttivi, a garanzia della sua validazione e applicazione ufficiale. È, inoltre, soggetto a riesame periodico, almeno con cadenza annuale o in seguito a eventi rilevanti quali incidenti informatici, cambiamenti organizzativi o variazioni nell'esposizione ai rischi. Il riesame e l'aggiornamento delle politiche e delle procedure di sicurezza sono curati dal Referente per la Cybersicurezza supportato dal Team di Sicurezza Informatica, al fine di garantire il costante allineamento delle misure adottate alle esigenze dell'organizzazione e alla normativa vigente in materia di sicurezza informatica.