Città metropolitana di Milano

DECRETO DEL SINDACO METROPOLITANO

In Pubblicazione:	dal 28/10/2026 al 11/11/2026
Repertorio Generale:	308/2026 del 28/10/2026
Protocollo:	192268/2026
Titolario/Anno/Fascicolo:	3.6/2026/10
Proponente:	CONSIGLIERE DELEGATO FRANCESCO VASSALLO
Materia:	CAMPUS DIGITALE
Oggetto:	APPROVAZIONE DELLA POLITICA DI SICUREZZA INFORMATICA E DEI DOCUMENTI ATTUATIVI PER L'ADEMPIMENTO DEGLI OBBLIGHI DI CUI AGLI ARTICOLI 23, 24, E 25 DEL D. LGS. 4 SETTEMBRE 2024, N. 138 (DECRETO NIS) IN QUALITÀ DI SOGGETTO IMPORTANTE.

DOCUMENTI CON IMPRONTE:

Documento 1 *2916_18159^DecretoFirmato.pdf*

3e8a42d32de232f1dbcbb2a69815b2ecb0b8de2c213503abb02ed176c7844c8e

Città metropolitana di Milano

DECRETO DEL SINDACO METROPOLITANO

Fascicolo 3.6/2026/10

Oggetto: Approvazione della Politica di sicurezza informatica e dei documenti attuativi per l'adempimento degli obblighi di cui agli articoli 23, 24, e 25 del D. Lgs. 4 settembre 2024, n. 138 (decreto NIS) in qualità di soggetto importante.

IL SINDACO METROPOLITANO

Assistito dal Segretario Generale

VISTA la proposta di decreto redatta all'interno;
VALUTATI i presupposti di fatto e le ragioni giuridiche a fondamento dell'adozione del presente atto in relazione alle risultanze dell'istruttoria;
VISTA la Legge n. 56/2014;
VISTE le disposizioni recate dal T.U. in materia di Comuni, approvate con D.Lvo 267/2000, per quanto compatibili con la Legge n. 56/2014;
VISTO lo Statuto della Città metropolitana ed in particolare l'art. 19 comma 2;
ACQUISITI i pareri di regolarità tecnica e di regolarità contabile espressi dai Dirigenti competenti, ai sensi dell'art. 49 del T.U. approvato con D.Lvo 267/2000;

DECRETA

1) di approvare la proposta di provvedimento redatta all'interno, dichiarandola parte integrante del presente atto;
2) di incaricare i competenti Uffici di provvedere agli atti consequenziali;
3) di incaricare il Segretario Generale dell'esecuzione del presente decreto.

Letto, approvato e sottoscritto

IL SINDACO	IL SEGRETARIO GENERALE

Documento informatico firmato digitalmente ai sensi del T.U. 445/2000 e del D.Lgs 82/2005 e rispettive norme collegate.

Città metropolitana di Milano

PROPOSTA
di decreto del Sindaco Metropolitano

Fascicolo 3.6\2026\10

DIREZIONE PROPONENTE Direzione Generale

Oggetto: Approvazione della Politica di sicurezza informatica e dei documenti attuativi per l'adempimento degli obblighi di cui agli articoli 23, 24 e 25 del D.Lgs. 4 settembre 2024, n. 138 (decreto NIS), in qualità di soggetto importante.

IL SINDACO METROPOLITANO

Visto il Decreto n. 148/2023, atti n. 91650/2023/1.9/2023/1, con il quale è stata conferita al Vicesindaco metropolitano Francesco Vassallo la delega, fra le altre, alle materie "Campus Digitale, Comunicazione, Personale e Organizzazione";

PREMESSO che:

- con Determinazione del Direttore Generale dell'ACN n. 136430 del 12 aprile 2025, comunicata all'Ente con nota del 14 aprile 2025, la Città metropolitana di Milano è stata individuata quale soggetto importante ai sensi del decreto NIS, nella tipologia "Città metropolitane" (Allegato III);

- con decreto del Sindaco metropolitano R.G. n. 128/2025 del 22/05/2025 il Dipartimento Transizione digitale è stato individuato quale struttura competente ai sensi dell'art. 8, comma 1, della legge n. 90/2024 e si è dato atto che le funzioni che l'art. 23 del decreto NIS attribuisce agli organi di amministrazione e agli organi direttivi sono esercitate, rispettivamente, dal Vicesindaco, quale consigliere delegato, e dal Direttore Generale;

ATTESO che il Dipartimento Transizione digitale risulta nell'organigramma dell'Ente alla diretta dipendenza del Direttore Generale e, come definito da ultimo con decreto del Sindaco metropolitano R.G. n. 287/2025 del 31/10/2025, ha fra i propri ambiti di competenza la cybersicurezza dell'Ente;

VISTO il decreto del Sindaco metropolitano R.G. n. 59/2026 del 04/03/2026 con il quale la dott.ssa Ester Anzalone, Direttrice del Dipartimento Transizione digitale, è stata nominata Referente per la cybersicurezza, Responsabile per la transizione digitale e Responsabile della

protezione dei dati personali, ed è registrata sul Portale ACN quale punto di contatto NIS dell'Ente;

VISTO che il Dipartimento Transizione digitale, ai fini dell'adeguamento dell'Ente agli obblighi del decreto NIS, ha provveduto alla ricognizione dei sistemi informativi e di rete rilevanti, all'analisi dello stato di attuazione delle misure di sicurezza di base e alla valutazione dei rischi, predisponendo tutti i documenti previsti dalla normativa che definiscono l'organizzazione per la sicurezza, il metodo e gli esiti della valutazione del rischio, il trattamento dei rischi, la gestione delle vulnerabilità, il piano di adeguamento alle misure di base, la continuità operativa, il disaster recovery e la gestione delle crisi, la formazione e la gestione degli incidenti con la notifica al CSIRT Italia ;

CONSIDERATO che i documenti prevedono che i registri e gli elenchi operativi a supporto (registro dei rischi e delle vulnerabilità, ruoli e responsabilità, contatti, obiettivi di ripristino, comitato di crisi, registro degli incidenti) siano tenuti e aggiornati dal Dipartimento Transizione digitale, e che le modifiche non sostanziali ai documenti siano approvate dalla Direttrice del Dipartimento, mentre le modifiche sostanziali e i riesami periodici siano sottoposti agli organi di amministrazione e direttivi;

CONSIDERATO che:

- l'approvazione dei documenti da parte degli organi di amministrazione e direttivi costituisce adempimento dell'obbligo di cui all'art. 23, comma 1, lettera a), del decreto NIS ed è condizione per la loro efficacia nei confronti di tutte le strutture dell'Ente;

- l'adozione dei documenti è finalizzata all'adempimento degli obblighi relativi alle misure di sicurezza di base nei termini stabiliti dalla Determinazione ACN n. 379907/2025, come aggiornata e integrata dalla Determinazione n. 127434/2026, e di disporre di un riferimento unico per l'attuazione e il monitoraggio delle misure, tutelando la continuità dei servizi resi a cittadini, Comuni e imprese;

- i documenti contengono informazioni sulle vulnerabilità e sull'assetto dei sistemi informativi e di rete dell'Ente la cui diffusione potrebbe pregiudicarne la sicurezza, e pertanto, ad eccezione della Politica di sicurezza informatica, non sono destinati alla pubblicazione;

- il Direttore Generale, in qualità di organo direttivo ai sensi dell'art. 23 del decreto NIS, ha esaminato i documenti predisposti dal Dipartimento Transizione digitale e, con la sottoscrizione della presente proposta, li approva per quanto di competenza e ne propone l'approvazione con il presente decreto, esprimendo il parere di regolarità tecnica;

RICHIAMATI gli atti di programmazione finanziaria dell'Ente (DUP e Bilancio di Previsione) e di gestione (PEG e PIAO);

VISTI i documenti dei quali si propone l'approvazione, elencati ai punti 1 e 2 del dispositivo;

VISTI:

- il D.lgs. 4 settembre 2024, n. 138, recante "Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148" (di seguito decreto NIS);

- l'art. 23, comma 1, del D.lgs. 4 settembre 2024, n. 138, ai sensi del quale gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e dei soggetti importanti approvano le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica adottate ai sensi dell'art. 24, sovrintendono all'implementazione degli obblighi in materia di gestione del rischio e di notifica degli incidenti e sono responsabili delle relative violazioni, e il comma 2 del medesimo articolo, che prevede per gli stessi organi l'obbligo di seguire una formazione in materia di sicurezza informatica e di promuovere la formazione dei dipendenti;

- l'art. 24 del D.lgs. 4 settembre 2024, n. 138, relativo alle misure tecniche, operative e organizzative per la gestione dei rischi per la sicurezza dei sistemi informativi e di rete, e l'art. 25, relativo agli obblighi di notifica degli incidenti significativi al CSIRT Italia;

- la Determinazione del Direttore Generale dell'Agenzia per la cybersicurezza nazionale (ACN) n. 379907/2025, che stabilisce le specifiche di base per l'adempimento degli obblighi di cui agli articoli 23, 24, 25, 29 e 32 del decreto NIS e, in particolare, l'Allegato 1 (misure di sicurezza di base per i soggetti importanti) e l'Allegato 3 (incidenti significativi di base per i soggetti importanti);

- la Determinazione del Direttore Generale dell' ACN n. 127434 del 13 aprile 2026, che aggiorna e integra la Determinazione n. 379907/2025 in materia di termini di adempimento, confermando per i soggetti inseriti nell' elenco nel 2025 i termini già previsti;

- la Determinazione del Direttore Generale dell' ACN n. 127437 del 13 aprile 2026, relativa alle modalità di utilizzo del Portale ACN, all' elencazione dei fornitori rilevanti e alla designazione del referente CSIRT;

- la legge 28 giugno 2024, n. 90, recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici", e in particolare l'art. 8;

VISTI altresì:
- la Legge 56/2014;
- le disposizioni recate dal T.U. in materia di Comuni, approvate con Decreto Lgs.18.08.2000 n. 267 "Testo Unico delle leggi sull'ordinamento degli Enti Locali", per quanto compatibili con la Legge n.56/2014;
- lo Statuto della Città metropolitana di Milano;

D E C R E T A

1) di approvare la Politica di sicurezza informatica per l'adempimento degli obblighi di cui agli articoli 23, 24 e 25 del D.Lgs. n. 138/2024 (decreto NIS), in qualità di soggetto importante, già approvata contestualmente dal Direttore Generale in qualità di organo direttivo con la sottoscrizione della proposta del presente provvedimento, come da Allegato A: CMM-NIS-POL-00 Politica di sicurezza informatica, versione 1.0, quale parte integrante del presente provvedimento;

2) di approvare, ai sensi dell'art. 23 del D.Lgs. 138/2024, i seguenti Allegati conservati in atti, già approvati contestualmente dal Direttore Generale in qualità di organo direttivo con la sottoscrizione della proposta del presente provvedimento:

- Allegato B: CMM-NIS-POL-b Organizzazione per la sicurezza informatica, versione 1.0;
- Allegato C: CMM-NIS-PIA-a1 Valutazione del rischio, versione 1.0;
- Allegato D: CMM-NIS-PIA-a2 Piano di trattamento del rischio, versione 1.0;
- Allegato E: CMM-NIS-PIA-g Piano di gestione delle vulnerabilità, versione 1.0;
- Allegato F: CMM-NIS-PIA-d Piano di adeguamento alle misure di sicurezza, versione 1.0;
- Allegato G: CMM-NIS-PIA-h Piano di continuità operativa, disaster recovery e gestione delle crisi, versione 1.0;
- Allegato H: CMM-NIS-PIA-k Piano di formazione, versione 1.0;
- Allegato I: CMM-NIS-PIA-p Piano di gestione degli incidenti e notifica al CSIRT Italia, versione 1.0;

3) di dare atto che il Vicesindaco, che sottoscrive il presente decreto in forza della delega di cui al decreto n. 148/2023, esercita le funzioni di organo di amministrazione ai sensi dell'art. 23 del D.Lgs. 138/2024, come stabilito dal decreto del Sindaco metropolitano R.G. n. 128/2025, e che con il presente decreto risultano pertanto approvati i documenti da parte di entrambi gli organi di amministrazione e direttivi;

4) di dare atto che i registri e gli elenchi operativi richiamati nei documenti di cui al punto 1 sono tenuti e aggiornati dal Dipartimento Transizione digitale e che le modifiche non sostanziali ai documenti sono approvate dalla Direttrice del Dipartimento, mentre le modifiche sostanziali e i riesami periodici sono sottoposti all'approvazione degli organi di amministrazione e direttivi;

5) di dare atto che gli organi di amministrazione e direttivi sovrintendono all'attuazione dei documenti approvati, anche sulla base delle relazioni periodiche predisposte dal Dipartimento Transizione digitale, e partecipano alla formazione prevista dal Piano di formazione (Allegato H), ai sensi dell'art. 23, comma 2, del D.lgs. 138/2024;

6) di demandare alla Direttrice del Dipartimento Transizione digitale tutti i successivi adempimenti per l'esecuzione del presente decreto, ivi compresa la pubblicazione del presente provvedimento in Amministrazione Trasparente ai sensi dell'art. 12- comma 1 del D.lgs. 33/2013;

7) di demandare alla Direttrice del Dipartimento Transizione digitale la comunicazione dei documenti approvati alle strutture dell'Ente anche con la pubblicazione della Politica di sicurezza informatica sulla intranet e il monitoraggio dell'attuazione delle misure;

8) di dare atto che il presente decreto non comporta riflessi diretti o indiretti sulla situazione economico-finanziaria o sul patrimonio dell'Ente e pertanto non è dovuto il parere di regolarità contabile;

9) di dare atto che il presente procedimento, con riferimento all'Area funzionale di appartenenza, non è classificato a rischio.

PARERE DI REGOLARITÀ TECNICA/AMMINISTRATIVA
(inserito nell'atto ai sensi dell'art. 49 del TUEL approvato con D.lgs. n. 267/00)

☒ Favorevole

☐ Contrario

SI DICHIARA CHE L'ATTO NON COMPORTA RIFLESSI DIRETTI O INDIRETTI SULLA SITUAZIONE ECONOMICO-FINANZIARIA O SUL PATRIMONIO DELL'ENTE E PERTANTO NON È DOVUTO IL PARERE DI REGOLARITÀ CONTABILE

☒

(inserito nell'atto ai sensi dell'art. 49 del TUEL approvato con D.Lgs. 267/00
e dell'art. 11 del Regolamento sul Sistema dei Controlli Interni)

IL DIRETTORE GENERALE
Antonio Sebastiano Purcaro

*Documento informatico firmato digitalmente ai sensi del T.U. 445/2000 e del D.Lgs 82/2005 e rispettiv*e norme collegate.

ALLEGATO A

Città metropolitana di Milano

Dipartimento Transizione Digitale

Politica di sicurezza informatica

CMM-NIS-POL-00 · versione 1.0

ai sensi del D.Lgs. 4 settembre 2024, n. 138 e della Determinazione ACN n. 379907/2025

Approvato con decreto n. … del …

SCHEDA DEL DOCUMENTO

Codice	CMM-NIS-POL-00
Titolo	Politica di sicurezza informatica
Versione e data	1.0 del 19/10/2026
Stato	Prima versione, in approvazione.
Perimetro di applicazione	Città metropolitana di Milano – sistemi informativi e di rete, con priorità per i sistemi rilevanti
Requisiti ACN	GV.PO-01 (punti 1-3); GV.PO-02; ambiti a)–p) della Tabella 1 dell'Allegato 1
Allegati	Allegato A – Corrispondenza tra ambiti, misure e documenti; Allegato B – Requisiti di sicurezza per i fornitori ICT
Classificazione	Uso interno

Iter di redazione e approvazione

Fase	Struttura / ruolo	Data e riferimento
Redazione	Dipartimento Transizione Digitale	19/10/2026
Verifica	Servizio Coordinamento sicurezza, service desk e procurement IT (referente CSIRT) e responsabili di ambito	21/10/2026
Istruttoria	Direttrice del Dipartimento Transizione Digitale	23/10/2026
Proposta e parere di regolarità tecnica	Direttore generale	Contenuti nel decreto R.G. n. .../2026 del .../10/2026
Approvazione	Direttore generale (organo direttivo), con la sottoscrizione della proposta; Vicesindaco (organo di amministrazione)	Decreto del Sindaco metropolitano R.G. n. .../2026 del .../10/2026
Decorrenza	Dalla data di approvazione	

Storico delle revisioni

Versione	Data	Descrizione delle modifiche	Redatto da
1.0	23/10/2026	Prima emissione	Dipartimento Transizione Digitale

INDICE

Definizioni 4
1. Aspetti generali 4
1.1. Introduzione 4
1.2. Obiettivo e ambito di applicazione 4
1.3. Fonti normative 4
2. Principi 5
3. Rapporto con gli altri documenti 5
4. Regole per ambito 5
4.1. Gestione del rischio (ambito a) 5
4.2. Ruoli e responsabilità (ambito b) 6
4.3. Affidabilità delle risorse umane (ambito c) 6
4.4. Conformità e audit di sicurezza (ambito d) 6
4.5. Catena di approvvigionamento (ambito e) 6
4.6. Gestione degli asset (ambito f) 6
4.7. Gestione delle vulnerabilità (ambito g) 7
4.8. Continuità operativa, ripristino e crisi (ambito h) 7
4.9. Identità digitali, autenticazione e controllo degli accessi (ambito i) 7
4.10. Sicurezza fisica (ambito j) 7
4.11. Formazione e consapevolezza (ambito k) 7
4.12. Sicurezza dei dati (ambito l) 8
4.13. Sviluppo, configurazione, manutenzione e dismissione (ambito m) 8
4.14. Protezione delle reti e delle comunicazioni (ambito n) 8
4.15. Monitoraggio degli eventi di sicurezza (ambito o) 8
4.16. Gestione degli incidenti, risposta e ripristino (ambito p) 8
5. Eccezioni 9
6. Approvazione e comunicazione 9
7. Formazione e sensibilizzazione 9
8. Violazioni 9
9. Revisione e aggiornamento 9
Allegato A – Corrispondenza tra ambiti, misure e documenti 9
Allegato B – Requisiti di sicurezza per i fornitori ICT 10
B.1 Classificazione dei fornitori 10
B.2 Requisiti contrattuali 10

DEFINIZIONI

Termine	Definizione
Sistemi rilevanti	Sistemi informativi e di rete individuati dall'ente ai sensi della misura GV.OC-04, elencati nell'Allegato A del documento CMM-NIS-PIA-a1.
DTD	Dipartimento Transizione Digitale.
Servizio Coordinamento sicurezza	Servizio Coordinamento sicurezza, service desk e procurement IT del DTD.
Organi	Organi di amministrazione e direttivi ai fini NIS individuati con decreto R.G. 128/2025: Vicesindaco e Direttore generale.
ACN / CSIRT Italia	Agenzia per la Cybersicurezza Nazionale e il suo Computer Security Incident Response Team, destinatario delle notifiche degli incidenti significativi.
Politica	Insieme di principi e regole approvati dagli organi, che orientano procedure e piani.
Procedura	Documento operativo che descrive come si attua una regola, chi fa cosa e con quali strumenti.
Fornitore rilevante (Tier 1)	Fornitore classificato ad alta criticità secondo i criteri dell'Allegato B.

1. ASPETTI GENERALI

1.1. INTRODUZIONE

La politica stabilisce i principi e le regole con cui la Città metropolitana di Milano protegge i propri sistemi informativi e di rete e i dati che tratta. Copre i sedici ambiti indicati dalla Tabella 1 dell'Allegato 1 alla Determinazione ACN n. 379907/2025 ed è il riferimento per tutti i piani e le procedure di sicurezza.[1]

1.2. OBIETTIVO E AMBITO DI APPLICAZIONE

Si applica a tutti i sistemi informativi e di rete dell'ente, in cloud o nelle sedi, con priorità per i sistemi rilevanti; a tutto il personale, agli amministratori, ai collaboratori, agli stagisti e ai volontari del servizio civile; ai fornitori che accedono ai sistemi o ai dati dell'ente, per i quali le regole sono rese vincolanti tramite i contratti.

1.3. FONTI NORMATIVE

- D.Lgs. 4 settembre 2024, n. 138 (decreto NIS), in particolare artt. 23, 24 e 25.
- Determinazione ACN n. 379907/2025, Allegato 1 – misure di sicurezza di base per i soggetti importanti – e Allegato 3 – incidenti significativi di base.
- ACN, Linee guida NIS – Specifiche di base – Guida alla lettura.
- Legge 28 giugno 2024, n. 90 (disposizioni in materia di rafforzamento della cybersicurezza nazionale).
- Regolamento (UE) 2016/679 (GDPR).
- D.Lgs. 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale).
- D.Lgs. 31 marzo 2023, n. 36 (Codice dei contratti pubblici).
- Legge 20 maggio 1970, n. 300, art. 4 (impianti e strumenti di controllo).

[1] Requisito GV.PO-01, punti 1 e 2: politiche di sicurezza per gli ambiti della Tabella 1.

2. PRINCIPI

- **Responsabilità degli organi:** gli organi approvano la politica e ne sovrintendono l'attuazione; la Direttrice del DTD ne cura l'applicazione.
- **Proporzionalità al rischio:** le misure sono commisurate al rischio valutato con il metodo di CMM-NIS-PIA-a1.
- **Minimo privilegio:** ognuno accede solo a ciò che serve per il proprio lavoro.
- **Sicurezza fin dalla progettazione:** il DTD è coinvolto fin dall'inizio in ogni acquisto o progetto ICT, anche dei Settori.
- **Nessun sistema fuori dall'inventario:** ogni sistema, servizio cloud o fornitore ICT è noto al DTD.
- **Segnalare sempre:** chiunque noti un'anomalia la segnala subito; nessuno è sanzionato per una segnalazione in buona fede.
- **Tracciabilità:** decisioni, eccezioni e verifiche sono documentate.

3. RAPPORTO CON GLI ALTRI DOCUMENTI

La politica è attuata dai piani del pacchetto NIS e dalle procedure indicate nell'Allegato A. Restano in vigore, per quanto compatibili, e sono allineati alla politica al primo riesame:

- il **Disciplinare per l'utilizzo dei servizi informatici** e di comunicazione telematica, approvato con decreto del Sindaco metropolitano R.G. 230/2024 del 24/09/2024, che contiene le regole d'uso degli strumenti ICT rivolte al personale. Al primo riesame va allineato alla presente politica, in particolare estendendo a qualunque incidente di sicurezza l'obbligo di segnalazione al DTD, oggi previsto per gli incidenti che possono comportare una violazione di dati personali;
- il documento **Misure minime di sicurezza ICT**, versione 1 del 28/12/2017, adottato ai sensi della circolare AgID n. 2/2017.[2] Molti impegni assunti allora (politiche per configurazioni standard, aggiornamenti, vulnerabilità, utenze amministrative, accessi remoti) trovano attuazione nella presente politica e nei documenti del pacchetto NIS. Il documento non è stato più aggiornato: il suo aggiornamento è previsto entro giugno 2027, in coordinamento con il Manuale di gestione documentale.

4. REGOLE PER AMBITO

4.1. GESTIONE DEL RISCHIO (AMBITO A)

- L'ente mantiene l'elenco dei sistemi rilevanti, collegato ai servizi categorizzati sul portale ACN, e lo aggiorna a ogni variazione significativa.
- Il rischio è valutato almeno ogni due anni e dopo incidenti significativi o cambiamenti rilevanti, anche con riferimento ai fornitori.
- Ogni rischio non accettabile ha un trattamento con responsabile e data; i rischi residui sono accettati in modo motivato dai soggetti indicati in CMM-NIS-PIA-a1.

Documenti attuativi: CMM-NIS-PIA-a1; CMM-NIS-PIA-a2.[3]

[2] Il documento è riservato e non è allegato alla presente politica.

[3] Requisiti GV.OC-04, GV.RM-03, ID.RA-05, ID.RA-06.

4.2. Ruoli e responsabilità (ambito b)

- Ruoli, responsabilità e sostituti sono definiti in CMM-NIS-POL-b e riesaminati almeno ogni due anni.
- L'elenco del personale con ruoli di sicurezza è mantenuto aggiornato insieme ai ruoli sul portale ACN.

Documenti attuativi: CMM-NIS-POL-b.[4]

4.3. Affidabilità delle risorse umane (ambito c)

- Il personale con accesso privilegiato ai sistemi rilevanti, interno o dei fornitori, è individuato nominativamente dopo una valutazione di esperienza, capacità e affidabilità.
- Gli amministratori di sistema sono nominati con atto individuale; l'elenco è riesaminato almeno una volta l'anno.

Documenti attuativi: CMM-NIS-POL-b, capitolo 5.[5]

4.4. Conformità e audit di sicurezza (ambito d)

- La politica è riesaminata almeno una volta l'anno e quando cambiano norme, rischi o organizzazione.
- Lo stato di attuazione è seguito con il Piano di adeguamento; la Direttrice riferisce agli organi ogni sei mesi.

Documenti attuativi: CMM-NIS-PIA-d.[6]

4.5. Catena di approvvigionamento (ambito e)

- Per ogni acquisto ICT con possibili impatti sui sistemi il RUP coinvolge il DTD dalla fase di progettazione, anche con convenzioni o centrali di committenza.
- Il fornitore è classificato Tier 1 o Tier 2 secondo l'Allegato B; bandi, contratti e convenzioni includono i requisiti di sicurezza dell'Allegato B, salvo motivate e documentate ragioni, nel qual caso il rischio è trattato con misure compensative.
- Il Registro dei fornitori e dei contratti ICT è aggiornato a ogni affidamento, rinnovo o cessazione; per i fornitori Tier 1 il rischio è valutato e la conformità verificata almeno una volta l'anno.

Documenti attuativi: Registro dei fornitori e dei contratti ICT; Allegato B.[7]

4.6. Gestione degli asset (ambito f)

- L'ente mantiene inventari aggiornati di apparati (compresi rete, dispositivi mobili e IoT), software e applicazioni (compresi API e software open source) e servizi dei fornitori, compresi quelli cloud.
- Ogni nuovo sistema o servizio è registrato prima della messa in produzione, con il relativo responsabile.

Documenti attuativi: catalogo delle applicazioni; inventari di rete e postazioni; Registro fornitori.[8]

[4]Requisiti GV.RR-02.
[5]Requisiti GV.RR-04.
[6]Requisiti GV.PO-01, GV.PO-02, ID.IM-01.
[7]Requisiti GV.SC-01, GV.SC-02, GV.SC-04, GV.SC-05, GV.SC-07.
[8]Requisiti ID.AM-01, ID.AM-02, ID.AM-04.

4.7. Gestione delle vulnerabilità (ambito g)

- Le segnalazioni del CSIRT Italia e delle altre fonti sono gestite con un flusso unico, tracciato e assegnato.
- Le vulnerabilità sono risolte nei tempi fissati per gravità, oppure mitigate o accettate in modo motivato.
- Almeno una volta l'anno si svolge un penetration test sui sistemi rilevanti.

Documenti attuativi: CMM-NIS-PIA-g.[9]

4.8. Continuità operativa, ripristino e crisi (ambito h)

- Per i sistemi rilevanti l'ente mantiene piani di continuità, di ripristino e di gestione delle crisi, approvati e riesaminati almeno ogni due anni, e li verifica con test periodici.
- Gli obiettivi di ripristino sono definiti dai responsabili dei servizi e verificati con i fornitori.

Documenti attuativi: CMM-NIS-PIA-h.[10]

4.9. Identità digitali, autenticazione e controllo degli accessi (ambito i)

- Le utenze sono censite, individuali e approvate; le utenze tecniche hanno un responsabile.
- Le utenze sono create, modificate e revocate su comunicazione tempestiva delle strutture del personale, compresi stagisti e servizio civile, e verificate almeno una volta l'anno.
- Le utenze amministrative sono distinte da quelle di uso quotidiano.
- L'autenticazione a più fattori è obbligatoria per l'accesso remoto e per i servizi cloud dell'ente; per i sistemi rilevanti è adottata in base al rischio.
- Gli accessi remoti, anche dei fornitori, avvengono solo tramite la VPN dell'ente; per ogni fornitore il referente interno indica sistemi e permessi; l'elenco dei sistemi accessibili da remoto è mantenuto aggiornato.

Documenti attuativi: procedura di gestione delle utenze da redigere; configurazioni VPN e firewall.[11]

4.10. Sicurezza fisica (ambito j)

- L'accesso ai locali tecnici e agli apparati dei sistemi rilevanti è consentito al solo personale autorizzato ed è registrato.
- Dove gli armadi di rete non possono essere protetti fisicamente, il rischio di accesso non autorizzato alla rete è compensato dal NAC; il rischio di danneggiamento fisico degli apparati resta e va trattato nel piano di trattamento del rischio.

Documenti attuativi: procedura di accesso ai locali tecnici da redigere.[12]

4.11. Formazione e consapevolezza (ambito k)

- Tutto il personale riceve formazione sulla sicurezza informatica; per organi, dirigenti, referente CSIRT, sostituti e amministratori di sistema sono previsti percorsi specifici.
- La partecipazione è registrata e verificata.

Documenti attuativi: CMM-NIS-PIA-k.[13]

[9] Requisiti ID.RA-01, ID.RA-08.
[10] Requisiti ID.IM-04.
[11] Requisiti PR.AA-01, PR.AA-03, PR.AA-05, PR.IR-01.
[12] Requisiti PR.AA-06.
[13] Requisiti PR.AT-01.

4.12. Sicurezza dei dati (ambito L)

- I dati su dispositivi portatili e supporti rimovibili sono cifrati; l'esecuzione automatica dei supporti è disabilitata e i supporti sono analizzati prima dell'uso.
- Le comunicazioni da e verso l'esterno dei sistemi rilevanti usano protocolli cifrati sicuri.
- Dati e configurazioni sono salvati periodicamente in coerenza con i piani di continuità; per i sistemi rilevanti esiste una copia offline o non modificabile.
- Nessun server è messo in produzione senza backup attivo.

Documenti attuativi: CMM-NIS-PIA-h, capitolo sul backup.[14]

4.13. Sviluppo, configurazione, manutenzione e dismissione (ambito M)

- Si installano solo software e sistemi operativi con aggiornamenti di sicurezza disponibili; le eccezioni sono motivate, compensate e hanno una data di dismissione.
- Gli aggiornamenti di sicurezza sono installati senza ingiustificato ritardo.
- Gli accessi remoti e privilegiati sono registrati; per i sistemi rilevanti i log sono raccolti in modo sicuro e possibilmente centralizzato, con tempi di conservazione definiti.
- Lo sviluppo del software segue pratiche di sviluppo sicuro, anche per i fornitori.

Documenti attuativi: CMM-NIS-PIA-g; linee guida di sviluppo sicuro da redigere.[15]

4.14. Protezione delle reti e delle comunicazioni (ambito N)

- I firewall sono mantenuti aggiornati e configurati in modo adeguato; le regole sono documentate e riesaminate.
- La rete è progressivamente segmentata; l'accesso alla LAN è consentito solo a dispositivi e utenti dell'ente.

Documenti attuativi: configurazioni di rete; progetto rete.[16]

4.15. Monitoraggio degli eventi di sicurezza (ambito O)

- Per i sistemi rilevanti l'ente dispone di strumenti per rilevare tempestivamente gli incidenti significativi e definisce i livelli di servizio attesi.
- Postazioni e server sono protetti da sistemi aggiornati di rilevamento del codice malevolo.

Documenti attuativi: CMM-NIS-PIA-p (livelli di servizio attesi).[17]

4.16. Gestione degli incidenti, risposta e ripristino (ambito P)

- Gli incidenti sono gestiti da un gruppo secondo il piano dedicato; gli incidenti significativi sono notificati al CSIRT Italia nei tempi dell'art. 25 del decreto NIS.
- Tutte le strutture e i fornitori segnalano subito al DTD qualunque incidente sui sistemi che gestiscono.
- L'ente informa utenti e pubblico quando opportuno o richiesto dall'ACN e ripristina i sistemi con procedure documentate.

Documenti attuativi: CMM-NIS-PIA-p.[18]

[14] Requisiti PR.DS-01, PR.DS-02, PR.DS-11.
[15] Requisiti PR.PS-02, PR.PS-04, PR.PS-06.
[16] Requisiti PR.IR-01.
[17] Requisiti DE.CM-01, DE.CM-09.
[18] Requisiti RS.MA-01, RS.CO-02, RC.RP-01.

5. ECCEZIONI

Una regola può non essere applicata solo per motivate ragioni tecniche o normative, documentate dal responsabile di ambito e approvate dalla Direttrice, con misure compensative e data di superamento. Le eccezioni sono registrate nel registro unico dei rischi e delle vulnerabilità (ALL-a1).

6. APPROVAZIONE E COMUNICAZIONE

La politica è approvata dagli organi di amministrazione e direttivi.[19] È pubblicata nella intranet, comunicata a tutte le strutture e richiamata nei contratti con i fornitori. Le regole che riguardano la registrazione e il monitoraggio delle attività del personale sono applicate nel rispetto dell'art. 4 della legge 300/1970.

7. FORMAZIONE E SENSIBILIZZAZIONE

Il personale con ruoli nell'attuazione del presente documento riceve una formazione specifica sui suoi contenuti, secondo il Piano di formazione in materia di sicurezza informatica (CMM-NIS-PIA-k).

8. VIOLAZIONI

La violazione delle disposizioni del presente documento da parte del personale è valutata secondo il Codice di comportamento dell'ente e le norme disciplinari vigenti; per i fornitori, secondo le clausole contrattuali.

9. REVISIONE E AGGIORNAMENTO

La politica è riesaminata almeno una volta l'anno e comunque in caso di incidenti significativi, variazioni organizzative, mutamenti dell'esposizione alle minacce o modifiche normative.[20] Il riesame è curato dal Servizio Coordinamento sicurezza e approvato dalla Direttrice; le modifiche sostanziali sono sottoposte agli organi.

ALLEGATO A – CORRISPONDENZA TRA AMBITI, MISURE E DOCUMENTI

Ambito	Misure ACN	Documento attuativo	Stato al 31/10/2026
a) Gestione del rischio	GV.OC-04, GV.RM-03, ID.RA-05, ID.RA-06	CMM-NIS-PIA-a1, PIA-a2	Approvato
b) Ruoli e responsabilità	GV.RR-02	CMM-NIS-POL-b	Approvato
c) Affidabilità risorse umane	GV.RR-04	CMM-NIS-POL-b	Approvato; nomine in corso
d) Conformità e audit	GV.PO-01, GV.PO-02, ID.IM-01	CMM-NIS-POL-00, PIA-d	Approvato
e) Catena di approvvigionamento	GV.SC-01, -02, -04, -05, -07	Allegato B; Registro fornitori	Approvato; clausole ai rinnovi
f) Asset	ID.AM-01, -02, -04	Inventari	In corso
g) Vulnerabilità	ID.RA-01, ID.RA-08	CMM-NIS-PIA-g	Approvato

[19] Requisito GV.PO-01, punto 3.

[20] Requisito GV.PO-02.

Ambito	Misure ACN	Documento attuativo	Stato al 31/10/2026
h) Continuità e crisi	ID.IM-04	CMM-NIS-PIA-h	Approvato
i) Identità e accessi	PR.AA-01, -03, -05; PR.IR-01	Procedura utenze	Da redigere (2027)
j) Sicurezza fisica	PR.AA-06	Procedura locali tecnici	Da redigere (2027)
k) Formazione	PR.AT-01	CMM-NIS-PIA-k	Approvato
l) Sicurezza dei dati	PR.DS-01, -02, -11	CMM-NIS-PIA-h	Approvato
m) Sviluppo e manutenzione	PR.PS-02, -04, -06	CMM-NIS-PIA-g; linee guida	Parziale
n) Reti	PR.IR-01	Configurazioni	Parziale
o) Monitoraggio	DE.CM-01, DE.CM-09	CMM-NIS-PIA-p	Approvato; SIEM da attivare
p) Incidenti	RS.MA-01, RS.CO-02, RC.RP-01	CMM-NIS-PIA-p	Approvato

ALLEGATO B – REQUISITI DI SICUREZZA PER I FORNITORI ICT

B.1 Classificazione dei fornitori

Il fornitore è classificato **Tier 1 (alta criticità)** se ricorre anche uno solo dei criteri seguenti; altrimenti è **Tier 2 (standard)**. La classificazione è riportata nel Registro dei fornitori e dei contratti ICT.

Criterio	Tier 1 – alta criticità	Tier 2 – standard
Accesso ai sistemi	Accesso diretto, remoto o fisico, a sistemi rilevanti, identità, rete o dati riservati	Accesso limitato a sistemi non rilevanti o nessun accesso
Impatto sulla continuità	Il fermo blocca un servizio rilevante (es. protocollo, firma, rete, posta)	Disservizi parziali recuperabili senza impatto sui servizi rilevanti
Dati trattati	Dati personali in quantità o dati riservati	Dati non personali o in quantità limitata
Sostituibilità	Fornitore unico o sostituibile in più di sei mesi	Sostituibile con procedura ordinaria
Ruolo nella catena	Gestisce l'infrastruttura per conto dell'ente o è subfornitore di un Tier 1	Fornitore autonomo

B.2 Requisiti contrattuali

Requisito	Tier 1	Tier 2
Notifica degli incidenti all'ente: pre-notifica entro 12 ore dalla conoscenza, notifica entro 48 ore, relazione finale entro 20 giorni; anche senza dati personali	Obbligatorio	Obbligatorio
Referente per la sicurezza e contatto raggiungibile fuori orario	Obbligatorio	Raccomandato
Elenco nominativo del personale con accessi; nomina ad amministratore di sistema; accesso solo via VPN dell'ente con MFA; revoca a fine incarico	Obbligatorio	Obbligatorio se ha accessi
Livelli di servizio di intervento e ripristino, con RTO e RPO	Obbligatorio	Raccomandato
Backup con copia offline o non modificabile; test di ripristino almeno annuale con verbale	Obbligatorio se gestisce sistemi o dati	—
Aggiornamenti di sicurezza nei tempi di CMM-NIS-PIA-g; nessun componente fuori supporto senza accordo	Obbligatorio	Obbligatorio
Conservazione dei log di accesso e sicurezza per almeno 12 mesi e messa a disposizione	Obbligatorio	—

Requisito	Tier 1	Tier 2
Diritto di verifica (audit) dell'ente o di un terzo incaricato	Obbligatorio	Raccomandato
Autorizzazione preventiva dei subfornitori e trasferimento degli stessi obblighi	Obbligatorio	Obbligatorio
Restituzione e cancellazione sicura dei dati a fine contratto; supporto al subentro	Obbligatorio	Obbligatorio

Per i contratti in essere, non modificabili prima del rinnovo, il DTD chiede ai fornitori Tier 1 un impegno scritto alla notifica degli incidenti; le prime occasioni di inserimento delle clausole sono i rinnovi di InfoCert (31/12/2026), CSI Piemonte (2027-2028) e il nuovo contratto Consip alla scadenza dell'attuale SGM2 (31/08/2028).

Città metropolitana di Milano

PARERE DEL SEGRETARIO GENERALE
sulla proposta di decreto del Sindaco Metropolitano

Fascicolo 3.6\2026\10

Oggetto della proposta di decreto:

Approvazione della Politica di sicurezza informatica e dei documenti attuativi per l'adempimento degli obblighi di cui agli articoli 23, 24, e 25 del D. Lgs. 4 settembre 2024, n. 138 (decreto NIS) in qualità di soggetto importante.

PARERE DEL SEGRETARIO GENERALE
(inserito nell'atto ai sensi del Regolamento sul sistema dei controlli interni)

[X] Favorevole

[ ] Contrario

IL SEGRETARIO GENERALE

Documento informatico firmato digitalmente ai sensi del T.U. 445/2000 e del D.Lgs 82/2005 e rispettive norme collegate.