AZIENDA SANITARIA LOCALE DI PESCARA
Via Renato Paolini, 47 – 65124 Pescara (PE)

DELIBERAZIONE DEL DIRETTORE GENERALE
AZIENDA SANITARIA LOCALE DI PESCARA

ANNO: 2026 N. 1374

Data 24/08/2026

OGGETTO: APPROVAZIONE DEI DOCUMENTI "REGOLAMENTO AZIENDALE IN MATERIA DI NOMINA E FUNZIONI DEGLI AMMINISTRATORI DI SISTEMA", "POLITICA AZIENDALE DI GESTIONE DEGLI INCIDENTI INFORMATICI" E "POLITICA AZIENDALE PER L'UTILIZZO DI DISPOSITIVI PERSONALI (BYOD)", NELL'AMBITO DEL SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI (SGSI) ADOTTATO DALLA ASL DI PESCARA CON DELIBERAZIONE N. 648 DEL 30/04/2026.

IL DIRETTORE GENERALE

OGGETTO: Approvazione dei documenti "Regolamento aziendale in materia di nomina e funzioni degli Amministratori di Sistema", "Politica aziendale di gestione degli incidenti informatici" e "Politica aziendale per l'utilizzo di dispositivi personali (BYOD)", nell'ambito del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) adottato dalla ASL di Pescara con Deliberazione n. 648 del 30/04/2026.

PRESO ATTO della relazione del Dirigente proponente, Ing. Marco De Benedictis, che qui si riporta integralmente:

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GDPR);

VISTO il D.Lgs. 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali, come novellato dal D.Lgs. 10 agosto 2018, n. 101;

VISTO il Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, recante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", e successive modifiche e integrazioni;

VISTA la Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022 (c.d. Direttiva NIS2), relativa a misure per un livello comune elevato di cybersicurezza nell'Unione;

VISTO il D.Lgs. 4 settembre 2024, n. 138, di recepimento della Direttiva NIS2, ed in particolare:

- l'art. 23, che pone in capo agli organi di amministrazione e direttivi l'obbligo di approvare le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica e di vigilare sulla relativa attuazione;
- l'art. 24, che impone l'adozione di misure tecniche, operative ed organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza dei sistemi informativi e di rete;

VISTA la Legge 28 giugno 2024, n. 90, recante disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici;
VISTA la Determinazione ACN n. 379907/2025, efficace dal 15 gennaio 2026, recante le tipologie di incidenti significativi per i Soggetti Essenziali ed i relativi livelli di servizio attesi;
VISTA la Legge 20 maggio 1970, n. 300 (Statuto dei Lavoratori) ed in particolare l'art. 4, in materia di controlli a distanza e utilizzo di strumenti di lavoro;
VISTA la Deliberazione del Direttore Generale della ASL di Pescara n. 648 del 30/04/2026, con la quale è stata approvata la "Politica aziendale per la sicurezza dei sistemi, dei dati e delle informazioni", documento di governance generale del Sistema di Gestione della Sicurezza delle Informazioni (SGSI), nella quale si stabiliva che la medesima Politica sarebbe stata attuata e integrata da policy e documenti specifici di ambito, da adottarsi con successivi atti;

PREMESSO CHE:

- l'Azienda Sanitaria Locale di Pescara è qualificata quale Soggetto Essenziale ai sensi del D.Lgs. 138/2024, in ragione dell'erogazione di servizi sanitari essenziali alla popolazione e del trattamento di dati sanitari rientranti nelle categorie particolari di cui all'art. 9 del GDPR, ed è pertanto tenuta all'adozione delle misure di gestione del rischio cyber e degli assetti di governance previsti dalla normativa NIS2;
- con la sopra richiamata Deliberazione n. 648 del 30/04/2026 è stato approvato il documento di primo livello del SGSI aziendale, che definisce l'impianto generale delle politiche di sicurezza e demanda a documenti attuativi di ambito la disciplina di dettaglio delle singole aree di rischio, tra cui la gestione degli Amministratori di Sistema, la gestione degli incidenti di sicurezza informatica e l'utilizzo di dispositivi personali per finalità lavorative (BYOD);
- l'U.O.C. Sistemi Informativi, in raccordo con il Referente per la Cybersicurezza e con l'Ufficio Privacy e Sicurezza delle Informazioni, ha curato la predisposizione dei documenti attuativi in oggetto, coerentemente con l'impianto della Politica aziendale approvata con Deliberazione n. 648/2026 e con il quadro normativo vigente in materia di protezione dei dati personali e di cybersicurezza;

CONSIDERATO CHE:

- il **"Regolamento aziendale in materia di nomina e funzioni degli Amministratori di Sistema"** disciplina i criteri e le modalità di individuazione, nomina, valutazione e verifica degli Amministratori di Sistema operanti sull'infrastruttura informatica e sugli applicativi in uso presso l'Azienda, in attuazione del Provvedimento del Garante Privacy del 27/11/2008 e ss.mm.ii. e in coerenza con gli obblighi di gestione del rischio di cui agli artt. 23-24 del D.Lgs. 138/2024;
- la **"Politica aziendale di gestione degli incidenti informatici"** e la correlata **"Procedura aziendale di gestione degli incidenti informatici"** (documento che verrà adottato in seguito) definiscono, rispettivamente, i principi generali di governance e il processo operativo per l'identificazione, la classificazione, la gestione e la notifica degli incidenti di sicurezza, in attuazione degli obblighi di cui agli artt. 23-24 del D.Lgs. 138/2024 e in coordinamento con gli obblighi di notifica al Garante Privacy ai sensi dell'art. 33 del GDPR;
- la "**Politica aziendale per l'utilizzo di dispositivi personali (BYOD)"** disciplina condizioni, limiti e responsabilità connessi all'utilizzo di dispositivi personali per finalità lavorative, in coerenza con i principi di minimizzazione dei rischi per la riservatezza dei dati aziendali e di rispetto delle garanzie di cui all'art. 4 della L. 300/1970 in materia di controllo a distanza degli strumenti di lavoro;
- tutti i documenti sopra richiamati costituiscono attuazione e integrazione della Politica aziendale approvata con Deliberazione n. 648/2026, di cui condividono l'impianto sistematico e ai cui principi generali si conformano;

RITENUTO, per le motivazioni sopra esposte, necessario ed opportuno procedere all'approvazione formale dei tre documenti sopra richiamati, al fine di dare seguito al processo di completamento del quadro documentale del Sistema di Gestione della Sicurezza delle Informazioni aziendale e di garantire la piena conformità dell'Azienda agli obblighi derivanti dal D.Lgs. 138/2024 e dalla normativa di settore;

ACQUISITO il parere tecnico favorevole in merito espresso dal Dirigente proponente, ai sensi della Legge 7 Agosto 1990 n. 241 e s.m.i. che ne attesta la regolarità e la completezza;

DATO ATTO dell'attestazione resa dai competenti Responsabili in ordine alla regolarità amministrativo-contabile e tecnica del presente provvedimento:
1. Dirigente proponente nella sua qualità di Direttore della U.O.C. Sistemi Informativi;

ACQUISITI, per quanto di competenza, i pareri favorevoli espressi in merito dal Direttore Amministrativo d'Azienda e dal Direttore Sanitario d'Azienda;

DELIBERA

Per tutto quanto esposto in premessa:
1) di **APPROVARE** il dei tre documenti allegati:
- Regolamento aziendale in materia di nomina e funzioni degli Amministratori di Sistema;
- Politica aziendale di gestione degli incidenti informatici;
- Politica aziendale per l'utilizzo di dispositivi personali (BYOD);

al fine di dare seguito al processo di completamento del quadro documentale del Sistema di Gestione della Sicurezza delle Informazioni aziendale e di garantire la piena conformità dell'Azienda agli obblighi derivanti dal D.Lgs. 138/2024 e dalla normativa di settore;

2) di **DARE ATTO** che dal presente provvedimento non derivano oneri aggiuntivi a carico del Bilancio Aziendale;

3) di **DARE MANDATO** di trasmettere copia della presente deliberazione a:
- a) Direzione Strategica;
- b) Direzioni delle aree tecnologiche:
  - i. UOC Sistemi Informativi;
  - ii. UOC Ingegneria Clinica;
  - iii. UOC Servizi Tecnici e Manutentivi;
  - iv. UOSD Progettazioni e Nuove Realizzazioni;
- c) Direttori di UOC e Responsabili di UOSD;
- d) Ufficio Privacy e Sicurezza delle Informazioni;
- e) UOC Acquisizione Beni e Servizi;
- f) UOC Dinamiche del Personale;
- g) UOS Formazione e Ricerca;
- h) UOS Risk Management;

4) di **DARE ATTO** che il presente atto, ai sensi dell'art.6 del regolamento interno approvato con Deliberazione 28.06.2012, numero 705, è immediatamente esecutivo;

5) di **DARE ATTO** che, ai sensi della Legge Regionale n. 10/2022 decorsi i termini di pubblicazione di cui al D.Lgs. n. 69/2009 il presente provvedimento, sarà soggetto a pubblicazione integrale

Politica aziendale per l'utilizzo di dispositivi personali (BYOD)

Revisioni Documento

Redazione, verifica e approvazione

Redazione	**M. D'Alessandro**
Verifica	**Direttore UOC Sistemi Informativi** **Responsabile Protezione Dati**
Approvazione	**Titolare del trattamento**

Storico revisioni

Versione	**Data**	**Autore**	**Note**
1.0.0	05/06/2026	M. D'Alessandro	Redazione prima bozza
1.0.1	01/07/2026	Davide De Luca	Revisione ufficio privacy
1.1	29/07/2026	M. D'Alessandro	Emissione

Lista di distribuzione

Destinatario	**Motivo**
Direttore Generale	Per competenza
Direttore Sanitario	
Direttore Amministrativo	
Ufficio Privacy e Sicurezza delle Informazioni	
Tutti i dipendenti	
Fornitori	Per quanto di competenza
Responsabile della Prevenzione della Corruzione e della Trasparenza	Per conoscenza

Sommario

1. Scopo

La presente Politica disciplina le modalità, le condizioni e le regole di comportamento con cui il personale della ASL di Pescara e i soggetti terzi autorizzati possono utilizzare i dispositivi di proprietà personale (laptop, smartphone, tablet) per accedere a risorse, servizi e sistemi informativi aziendali.

La ASL di Pescara, in accordo con la propria missione aziendale, considera il principio del "BYOD" ("Bring Your Own Device – Porta il tuo dispositivo") uno strumento prezioso per il raggiungimento di una piena mobilità e flessibilità operativa, e ne incoraggia l'uso.

La Politica persegue i seguenti obiettivi:

- definire le condizioni minime di sicurezza per l'accesso ai sistemi aziendali tramite dispositivi personali;
- tutelare l'integrità, la riservatezza e la disponibilità dei dati e delle informazioni trattate;
- assicurare il rispetto dei principi stabiliti dai regolamenti aziendali e dalle normative vigenti in materia di protezione dei dati personali e cybersicurezza;
- definire responsabilità chiare per tutti i soggetti coinvolti.

2. Campo di applicazione

La presente Politica si applica a tutti i dipendenti, collaboratori e/o soggetti terzi che, a qualsiasi titolo, accedono ai sistemi informativi aziendali della ASL di Pescara mediante dispositivi di loro proprietà o nella loro disponibilità privata.

I dispositivi di proprietà aziendale assegnati in uso esclusivo al dipendente sono disciplinati dalla Delibera n.23 del 12/01/2016, attualmente in corso di aggiornamento per il recepimento delle recenti normative in materia di cybersicurezza, e pertanto non rientrano nell'ambito della presente Politica.

3. Principi generali

La presente Politica si fonda sui seguenti principi generali:

- **Sicurezza e responsabilità**: l'uso dei dispositivi personali, incoraggiato e sostenuto dall'Azienda per i suoi innumerevoli vantaggi, introduce rischi specifici di sicurezza informatica e protezione dei dati. Tali rischi vanno mitigati attraverso buone prassi e comportamenti rigorosi e appropriati da parte dei dipendenti, regolamentati nel presente documento;
- **Proprietà e costi**: i costi di tutti i dispositivi personali, compresa la stipula dei contratto di utenza, i servizi di telefonia, gli aggiornamenti hardware software e le garanzie di manutenzione o di

sostituzione in caso di furto, sono a carico dei rispettivi proprietari. I costi dei dispositivi aziendali e dei relativi contratti d'uso sono a carico dell'azienda per tutti gli usi consentiti;

- **Proporzionalità**: le misure di sicurezza richieste sono stabilite in modo proporzionale al livello di rischio associato all'utilizzo di un determinato dispositivo e dei dati trattati;
- **Separazione logica**: i sistemi e i servizi aziendali acceduti tramite dispositivo personale non devono consentire la memorizzazione permanente di dati aziendali riservati sul dispositivo stesso, salvo casi specifici autorizzati;
- **Non invasività**: l'Azienda si impegna a non installare software di monitoraggio o controllo dell'attività del dipendente sui dispositivi personali.
- **Protezione dei dati**: la raccolta dei dati e dei log di utilizzo dei sistemi aziendali viene effettuata esclusivamente per le finalità previste dall'accordo sottoscritto per il trattamento dei dati, per le necessarie conformità normative in materia di cybersicurezza, nonché per tutte le attività connesse ad indagini delle Autorità Giudiziarie;

4. Modalità di utilizzo dei dispositivi personali

Il presente capitolo disciplina le modalità di utilizzo di dispositivi personali da parte del personale interno all'Azienda.

4.1. Condizioni di utilizzo

Il personale può avvalersi del proprio dispositivo personale (smartphone, tablet, PC) per accedere ai sistemi informativi aziendali nel rispetto delle seguenti condizioni:

- Accettazione della presente Politica, dei principi e delle responsabilità in essa contenuti e dei regolamenti correlati;
- Il dispositivo deve essere protetto da un metodo sicuro per il blocco automatico e lo sblocco dello schermo, come ad esempio codice PIN, passphrase o fattore biometrico;
- Il dispositivo deve essere dotato di un sistema operativo supportato dal produttore e con aggiornamenti di sicurezza applicati;
- Il dispositivo non deve essere stato sottoposto a procedure di sblocco non autorizzato (jailbreak / root) che compromettono i meccanismi di sicurezza del sistema operativo;
- Il dispositivo deve disporre di software di protezione da malware attivo e aggiornato, ove disponibile per lo specifico sistema operativo utilizzato.

4.2. Casi d'uso consentiti

L'utilizzo del dispositivo personale da parte del personale interno è consentito per le seguenti finalità:

- Autenticazione a più fattori (MFA) per l'accesso ai PC in dominio aziendale;
- Accesso alla posta elettronica aziendale tramite client webmail o applicazione installata sul PC, in modalità che non preveda la sincronizzazione persistente della casella sul dispositivo personale;
- Connessione alla rete aziendale tramite VPN per lo svolgimento dell'attività lavorativa in modalità di lavoro agile (smart working), in conformità alle disposizioni organizzative e contrattuali vigenti;
- Accesso ad applicativi aziendali di autenticazione tramite firma digitale;
- Accesso a portali di servizio interni e strumenti di condivisione (OneDrive, SharePoint, Teams);
- Ricezione di notifiche e codici OTP generati da applicazioni di autenticazione installate volontariamente sul dispositivo.

4.3. Obblighi del dipendente

Il personale interno che utilizza il proprio dispositivo per le finalità di cui alla sezione precedente è tenuto a:

- Mantenere il dispositivo aggiornato e in condizioni di sicurezza adeguate per tutta la durata dell'utilizzo;
- Non condividere con terzi le credenziali aziendali né consentire ad altri soggetti di accedere ai sistemi aziendali tramite il proprio dispositivo;
- Segnalare tempestivamente all'Help Desk Informatico qualsiasi evento che possa aver compromesso la sicurezza del dispositivo (furto, smarrimento, accesso non autorizzato, infezione da malware);
- Disconnettersi dai sistemi aziendali al termine di ogni sessione di utilizzo;
- Non conservare copie di dati aziendali riservati, dati sanitari o informazioni classificate nella memoria locale del dispositivo, in applicazioni personali, servizi cloud privati o supporti rimovibili non autorizzati;
- Consentire la revoca dell'accesso ai sistemi aziendali da parte della UOC Sistemi Informativi in caso di cessazione del rapporto di lavoro, variazione dei privilegi o necessità di sicurezza.

4.4. Divieti

I divieti di cui alla presente sezione sono da intendersi come tassativi. La loro violazione può comportare conseguenze disciplinari e, nei casi previsti dalla legge, responsabilità civili e penali.

È fatto espresso divieto al personale interno di:

- Conservare, scaricare o trasferire sul dispositivo personale tutte le informazioni trattate per lo svolgimento dell'attività lavorativa oltre la sessione di lavoro;

- Accedere ai sistemi aziendali tramite reti pubbliche non protette senza l'utilizzo della VPN aziendale;
- Installare sul dispositivo applicazioni di accesso remoto o condivisione dello schermo non autorizzate che potrebbero esporre attività, credenziali di accesso o dati contenuti nel dispositivo;
- Trasmettere informazioni aziendali a indirizzi di posta elettronica personali o sistemi di messaggistica esterni;
- Aggirare i meccanismi di autenticazione o i controlli di accesso dei sistemi aziendali;

4.5. Trattamento dei dati

Il trattamento dei dati aziendali mediante dispositivo personale è consentito esclusivamente nei limiti dell'autorizzazione ricevuta dal titolare del trattamento, funzionali all'erogazione del servizio e nel rispetto delle disposizioni già in uso presso l'ASL.

5. Normativa di riferimento

La presente Politica è redatta in conformità al quadro normativo vigente, tenendo conto delle seguenti fonti legislative nazionali ed eurounitarie, nonché delle principali linee guida e standard di settore:

Normativa nazionale

- **Legge 28 giugno 2024, n. 90**, *"Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici"*;
- **Decreto legislativo 4 settembre 2024, n. 134**, *"Attuazione della Direttiva (UE) 2022/2557 relativa alla resilienza dei soggetti critici e abrogazione della Direttiva 2008/114/CE"*;
- **Decreto legislativo 4 settembre 2024, n. 138**, *" 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"*;
- **Decreto-legge 21 settembre 2019, n. 105**, convertito con modificazioni dalla **Legge 18 novembre 2019, n. 133**, recante *"Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e disciplina dei poteri speciali nei settori strategici"*;
- **Direttiva del Presidente del Consiglio dei Ministri del 29 dicembre 2023**, *"Resilienza cibernetica del Paese – Protocolli di intesa per irrobustire la capacità di risposta agli incidenti informatici"*.
- **D.Lgs.196/2003** per come novellato dal D.Lgs.101/2018 e ss.mm.ii.

Normativa eurounitaria

- **Regolamento (UE) 2016/679**, *"Regolamento generale sulla protezione dei dati" (GDPR)*;
- **Direttiva (UE) 2022/2555**, *"Direttiva NIS2 sulla cybersicurezza", relativa a misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione europea*;

- **Direttiva (UE) 2022/2557**, *"Direttiva CER relativa alla resilienza dei soggetti critici"*, recepita con D.Lgs. 134/2024.

Linee guida e standard di settore

- **Linee guida dell'Agenzia per la Cybersicurezza Nazionale (ACN)**, in materia di cybersicurezza, notificazione degli incidenti, gestione del rischio e perimetro nazionale di sicurezza cibernetica;
- **Linee guida Agenzia per l'Italia Digitale (AgID)** sulla sicurezza informatica, la gestione dei dati, l'interoperabilità e la continuità operativa delle infrastrutture digitali pubbliche;
- **Norma UNI CEI ISO/IEC 27001:2022**, *"Tecnologie informatiche – Tecniche di sicurezza – Sistemi di gestione della sicurezza delle informazioni – Requisiti"*;
- **Norma UNI CEI ISO/IEC 27002:2022**, *"Tecnologie informatiche – Tecniche di sicurezza – Codice di buona pratica per i controlli di sicurezza delle informazioni"*;
- **Framework Nazionale per la Cybersecurity e la Data Protection (FNCS) - Edizione 2025 (v2.1)**, frutto della collaborazione tra il Centro di Ricerca CIS di Sapienza Università di Roma ed il Laboratorio Nazionale di Cybersecurity del CINI, con il supporto dell'ACN, come riferimento metodologico volontario.

6. Definizioni ed acronimi

In questa sezione vengono riportati i principali termini tecnici e gli acronimi utilizzati all'interno della presente Politica, al fine di garantirne una corretta e univoca interpretazione.

Definizioni

- TO DO

Acronimi

- TO DO

Regolamento aziendale in materia di nomina e funzioni degli Amministratori di Sistema

Revisioni Documento

Redazione, verifica e approvazione

Redazione	**M. D'Alessandro**
Verifica	**Direttore UOC Sistemi Informativi** **Responsabile Protezione Dati** **Privacy Manager**
Approvazione	**Titolare del trattamento**
Livello di riservatezza	**Uso Interno**

Storico revisioni

Versione	Data	Autore	Note
1.0	23/01/2025	M. D'Alessandro	Redazione prima bozza
1.0.1	30/01/2025	M. D'Alessandro	Correzioni e chiarimenti in Sez. 3 dopo prima revisione con Direttore S.I.
1.0.2	28/07/2025	M. D'Alessandro	Recepite note DPO in sez: • 2: riferimento a VPN • 3.2: segnalazione impedimenti • 4.3: formazione obbligatoria • 4.5: gestione credenziali • 4.6: disponibilità e pubblicazione elenchi • 5.1: FAQ Garante Privacy
1.0.3	25/09/2025	D. De Luca	Prodotta prima bozza del modello di incarico (Sez. 6.1)
1.0.4	29/09/2025	M. D'Alessandro	Revisione finale, integrazione e controllo di tutte le modifiche presenti nelle precedenti revisioni
1.0.5	07/10/2025	D. De Luca	Integrazione dei modelli, rimozione revisioni e commenti
1.0.6	30/10/2025	M. D'Alessandro L. Marino	Varie aggiunte, correzioni e integrazioni relative a ruoli, funzioni, responsabilità e limitazioni, nelle sezioni 3,4 e 5.
1.0.7	04/11/2025	M. D'Alessandro L. Marino D. De Luca	Varie aggiunte, correzioni e integrazioni relative a ruoli, funzioni, responsabilità e limitazioni e referente CSIRT
1.0.8	13/02/2026	M. D'Alessandro D. De Luca	Varie aggiunte, correzioni e integrazioni relative a ruoli, funzioni, responsabilità e limitazioni
1.0.9	04/03/2026	D. De Luca	Interventi atti ad applicare le indicazioni della UOS Selezione e Gestione del Rapporto di Lavoro
1.1	29/07/2026	M. D'Alessandro	Emissione

Lista di distribuzione

Destinatario	Motivo
Direttore Generale	Per competenza
Direttore Sanitario aziendale	
Direttore Amministrativo aziendale	
Ufficio Privacy e Sicurezza delle Informazioni	
Ai Soggetti Autorizzati al Trattamento con delega (SATD)	
Ai Fornitori	Per quanto di competenza
Responsabile della Prevenzione della Corruzione e della Trasparenza	Per conoscenza
Dirigente UOS Formazione	Per quanto di competenza

Sommario

1 Generalità

1.1 Finalità

Il presente Regolamento definisce le procedure per la nomina e l'attribuzione delle funzioni degli amministratori di sistema che operano sull'infrastruttura informatica e sugli applicativi in uso presso la ASL di Pescara. L'obiettivo è di garantire il rispetto degli obblighi in materia di protezione dei dati personali e di sicurezza informatica, stabilendo regole e misure specifiche per le attività svolte dal personale interno e da soggetti esterni con funzioni simili, anche se non esclusivamente tecniche o informatiche.

Gli indirizzamenti formulati nel presente documento costituiscono un insieme di misure minime la cui attuazione si rende necessaria per contenere entro limiti accettabili, stabiliti dagli organi direzionali in coerenza con le analisi del rischio di cybersecurity e protezione dei dati, il rischio di compromissioni della riservatezza, integrità e disponibilità dei dati personali trattati dal Titolare dei trattamenti e i rischi relativi alla sicurezza dell'infrastruttura informatica della ASL di Pescara. Tali misure potranno e dovranno essere incrementate qualora, in determinati contesti, siano richiesti livelli di protezione più elevati o qualora intervengano nuove normative specifiche.

In applicazione del principio di accountability (responsabilizzazione), la ASL di Pescara, in qualità di titolare del trattamento, documenta analiticamente e rende disponibili per verifiche interne e ispezioni esterne tutte le decisioni e misure tecniche e organizzative adottate per la gestione degli amministratori di sistema, garantendo tempestività e completezza nell'attuazione delle raccomandazioni ricevute dal DPO.

1.2 Normativa di riferimento

Il presente regolamento recepisce quanto previsto dalle seguenti normative:

- Provvedimento del Garante Privacy del 27/11/2008 e s.m.i. "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"
- Legge 23 dicembre 1993, n. 547 "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica"
- Codice Penale dello Stato Italiano
- LEGGE18 marzo 2008, n. 48. Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno.
- Provvedimento n.13 del Garante Privacy del 01/03/2007 (G.U. n. 58 del 10 marzo 2007) "Lavoro: le linee guida del Garante per posta elettronica e internet"
- Provvedimento del Garante Privacy del 2009 e s.m.i. "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"
- Regolamento UE 2016/679 (c.d. GDPR)
- Delibera n. 23/2016 della ASL di Pescara "Regolamento aziendale inerente le modalità di utilizzo della posta elettronica, di internet e degli strumenti informatici da parte del personale della azienda U.S.L. di Pescara".

- AGENZIA PER L'ITALIA DIGITALE CIRCOLARE 18 aprile 2017, n. 2/2017 Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)».
- D.Lgs. 196/2003 per come novellato dal D.Lgs. 101/2018
- Direttiva UE 2022/2555 recepita con D.lgs. 138/2024, c.d. Decreto NIS2
- LEGGE 28 giugno 2024, n. 90 Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici. (24G00108) (GU Serie Generale n.153 del 02-07-2024)

1.3 Definizioni ed acronimi

Termine/Abbreviazione	Definizione
Amministratore di Sistema (AdS)	Secondo quanto previsto nel Provvedimento del Garante Privacy "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" del 27/11/2008 e successive modifiche ed integrazioni (provvedimenti del 12/02/2009 e del 25/06/2009), con la definizione di "Amministratore di sistema" si individuano, in ambito informatico, figure professionali finalizzate alla gestione ed alla manutenzione di un impianto di elaborazione o di sue componenti. Vengono considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistema software complessi.
ACN	
CSIRT	
Dato personale **(Art. 4 co. 1 GDPR)**	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.
Trattamento **(Art. 4 co. 2 GDPR)**	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.
Titolare del trattamento **(Art. 4 co. 7 GDPR)**	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.
Responsabile del trattamento **(Art. 4 co. 8 GDPR)**	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

2 Definizione di Amministratore di Sistema

Il presente regolamento, in linea con il Provvedimento del Garante per la protezione dei dati personali e con la normativa vigente in materia di sicurezza informatica, identifica l'Amministratore di Sistema quale figura professionale dedicata alla gestione e alla manutenzione di sistemi di elaborazione con cui vengano effettuati trattamenti di dati personali.

Rientrano in questa ampia accezione tutte le figure chiamate a svolgere funzioni che comportano la concreta capacità di accedere, in modo privilegiato, a risorse del sistema informativo e a dati personali, anche qualora non siano preposte a operazioni che implicano una comprensione del dominio applicativo.

Vista tale classificazione si sottolinea che, in taluni contesti e per funzioni specifiche (es. amministrazione delle sole credenziali), può essere nominato Amministratore di Sistema anche personale (interno o esterno) non in possesso di competenze informatiche specialistiche. Si pensi ad esempio al personale medico o di supporto che è in possesso di credenziali di autenticazione privilegiate per la gestione di un software specifico di un Reparto, Unità o Organizzazione all'interno della ASL. Tali soggetti rientrano a tutti gli effetti nella definizione di "Credential Administrator" (si veda classificazione seguente) e saranno pertanto nominati Amministratori di Sistema dai propri responsabili designati.

Tra i sistemi oggetto della normativa rientrano:

- Sistemi di gestione delle basi di dati e di backup (es. DBMS, DB server, backup server)
- Software gestionali complessi (es. ERP, CRM)
- Sistemi operativi
- Infrastrutture di rete (es. router, switch) e software collegati (es. VPN)
- Apparati di fonia fissa e mobile
- Apparati di sicurezza (es. firewall, antivirus, SOC, SIEM)

Non sono considerati Amministratori di Sistema i soggetti che intervengono occasionalmente, ad esempio per attività di manutenzione straordinaria a seguito di guasti o malfunzionamenti.

Ai fini del presente documento, sono considerati Amministratori di Sistema le figure professionali che ricoprono uno o più dei seguenti ruoli, indipendentemente dal tipo di dati trattati e dalle specifiche competenze tecniche:

- **System Administrator**: responsabile della gestione e manutenzione di sistemi informatici, server e apparati hardware;
- **Database Administrator**: incaricato della gestione della struttura logica, dell'ottimizzazione delle prestazioni e del middleware dei sistemi di gestione delle basi di dati (DBMS);
- **Application Administrator**: responsabile della gestione di applicazioni, software e siti web;
- **Network Administrator**: incaricato della gestione delle reti informatiche e dei relativi apparati di comunicazione;
- **Security Administrator**: responsabile della gestione delle componenti e piattaforme hardware e software dedicate alla sicurezza informatica e delle reti;
- **Backup, Storage & Recovery Administrator**: incaricato della gestione dei supporti di memorizzazione e delle attività di backup e ripristino per sistemi hardware, software e basi di dati;
- **Credential Administrator**: responsabile della gestione delle credenziali di autenticazione e dei permessi di accesso ai sistemi informatici.

Non sono qualificabili come Amministratori di Sistema i soggetti che dispongono esclusivamente di privilegi limitati per svolgere attività ordinarie del proprio ruolo lavorativo, privi della capacità tecnica di accedere in modo generalizzato o esteso a dati personali non strettamente inerenti al proprio ambito di competenza.

3 Ruoli, funzioni e responsabilità

3.1 Funzioni, compiti e facoltà dell'Amministratore di Sistema

Tra i principali compiti e funzioni di natura tecnico/operativa che competono a un Amministratore di Sistema, ove del caso e compatibilmente con eventuali e comprovati vincoli o limitazioni di natura organizzativa, tecnica, economica o di performance, vi sono quelli riportati nell'elenco seguente. Gli ulteriori adempimenti di carattere generale, previsti dalla normativa, sono riportati nella Sez. 3.3 "Ruoli".

L'elenco seguente è da intendersi come non esaustivo e viene riportato a scopo puramente informativo ed esemplificativo. I compiti, i ruoli e le funzioni di ciascun Amministratore di Sistema sono specificati nell'atto di nomina individuale (v. Sez. 4).

- **Gestione e monitoraggio dei sistemi:** garantire il corretto funzionamento generale dei sistemi informatici, dei sottosistemi e delle applicazioni attraverso il monitoraggio dei messaggi di sistema e l'individuazione di anomalie o guasti.
- **Interventi di manutenzione:** diagnosticare e risolvere problemi tecnici, aggiornare periodicamente il sistema operativo, i driver e i software di base, e ottimizzare la configurazione del sistema per garantire prestazioni, sicurezza e affidabilità.
- **Backup e recupero dati:** verificare regolarmente l'esito dei salvataggi, effettuare il ripristino o il recupero dati quando necessario, e adottare misure per prevenire la perdita o distruzione dei dati.
- **Collaborazione con fornitori esterni:** segnalare necessità tecniche, coordinare interventi di manutenzione ordinaria o straordinaria, e informare utenti e strutture coinvolte.
- **Gestione degli utenti e dei permessi:** rilasciare credenziali, configurare account e profili di autorizzazione e mantenerle aggiornate in coerenza con le funzioni assegnate, secondo le indicazioni del Responsabile del Trattamento.
- **Configurazione e continuità operativa:** provvedere alla configurazione ottimale del sistema per garantire il migliore equilibrio fra le prestazioni erogate, la sicurezza operativa, la complessità e l'onerosità di gestione in ottica di massimizzare l'efficienza e la continuità operativa.
- **Interventi sui file system:** effettuare operazioni diagnostiche e di manutenzione sui file e sui file system per garantire la funzionalità del sistema.
- **Gestione dei log:** verificare la consistenza dei log applicativi in coerenza con quanto previsto dalle normative.
- **Audit e verifiche periodiche:** verificare periodicamente lo stato del sistema e la rispondenza di tutti i requisiti sopra elencati in coerenza con la normativa e con il proprio ruolo e le proprie funzioni.

3.2 Principi etici e responsabilità

Oltre ai compiti e alle funzioni tecnico/operative specificate nel paragrafo precedente, l'Amministratore di Sistema è tenuto ad osservare gli usuali principi di etica professionale quali trasparenza, affidabilità e senso di responsabilità. L'operato dell'Amministratore deve sempre avvenire nel pieno rispetto della normativa di cui alla Sez. 1.2.

Un Amministratore di Sistema si impegna:

- A segnalare e riportare, fin dal momento della sua nomina e per tutta la durata del suo operato, qualsiasi vincolo, impedimento o anomalia di natura organizzativa, economica, tecnica o di performance che abbia un impatto significativo sul corretto svolgimento delle proprie funzioni in relazione al sistema amministrato;
- A segnalare tempestivamente agli organi aziendali competenti (ove del caso, SATD, Dirigenti, DPO e referente CSIRT) ogni incidente di sicurezza o aumento del rischio relativo al sistema amministrato di cui si abbia conoscenza;
- A trattare i dati personali in modo lecito e secondo correttezza ed esclusivamente per gli scopi inerenti all'attività svolta nell'ambito delle proprie mansioni;
- A verificare, ove possibile e necessario, che tali dati siano esatti e, se lecito e necessario, ad aggiornarli;
- A verificare, ove possibile e necessario, che tali dati siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati;
- A trattare i dati rispettando le misure di sicurezza previste dalla normativa in materia di privacy e in particolare dalle indicazioni previste dal Codice di protezione in materia di dati personali (GDPR D.Lgs.196.2003 e s.m.i.);
- A non utilizzare a fini privati i dati cui accede;
- A non consentire a terzi non legittimati l'accesso ai dati ottenuti in ragione dell'espletamento dei propri compiti;
- A non divulgare eventuali dati riservati di cui venisse a conoscenza;
- A non interferire illegittimamente nel lavoro altrui;
- A non alterare illegittimamente o danneggiare i dati cui accede;
- A non effettuare controlli illegittimi sulla attività degli utenti del sistema.

Si richiama inoltre che, nello specifico contesto del Regolamento in oggetto, il ruolo di Amministratore di Sistema può costituire un'aggravante nel caso di commissione di uno dei seguenti reati:

- Accesso abusivo a sistema informatico o telematico (art. 615 ter del c.p.);
- Frode informatica (art. 640 ter del c.p.);
- Danneggiamento di informazioni, dati e programmi informatici (artt.635 bis e ter del c.p.) qualora sussista l'elemento soggettivo del dolo;
- Danneggiamento di sistemi informatici e telematici (artt. 635 quater e quinques del c.p.) qualora sussista l'elemento soggettivo del dolo.

3.3 Ruoli

Nella tabella seguente sono riportati sinteticamente i ruoli degli attori coinvolti nel processo di nomina e gestione degli Amministratori di Sistema (di seguito "AdS"), così come espressi dalla normativa vigente. I processi di nomina e gestione sono poi ulteriormente dettagliati nella Sezione 4.

Titolare del Trattamento	L'ASL di Pescara, intesa come intera organizzazione, è il titolare del trattamento.
Direttori e responsabili di UOC e Dipartimenti	Il Titolare del Trattamento demanda ai designati delle UU.OO.CC. e dei Dipartimenti di: • individuare e nominare, per i sistemi di cui fa uso, gli Amministratori di Sistema interni ed esterni in possesso delle necessarie competenze previste dalla normativa (v. Sez. 3, 4); • compilare ed aggiornare con cadenza annuale l'elenco degli Amministratori di Sistemi che si è provveduto a nominare; • predisporre le lettere di nomina sottoscritta dal Titolare del Trattamento, dal designato della UOC/Dipartimento e dall'Amministratore per "presa visone"; • predisporre le lettere di revoca nei casi in cui decadano i requisiti di nomina ad Amministratore di Sistema; • assicurare la registrazione e la conservazione dei log di accesso secondo i termini previsti; • effettuare, per la parte di propria competenza, verifiche periodiche sull'operato degli Amministratori di Sistema per rilevarne la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati; • informare la UOC Sistemi Informativi e l'Ufficio Privacy delle nomine/revoche ad Amministratori di Sistema effettuate. Il Titolare si impegna, per il tramite delle competenti funzioni aziendali (UOC Sistemi Informativi e UOS Formazione) a erogare tutti gli interventi formativi previsti dalla normativa in ambito tecnico, informatico, sanitario e di protezione dei dati.
Responsabile del trattamento (Art. 4 co. 8 GDPR)	Il Responsabile del Trattamento, che può essere una persona fisica o giuridica, pubblica o privata, è il soggetto che svolge attività di trattamento per conto del Titolare del Trattamento. Il titolare del trattamento designa obbligatoriamente un Responsabile del trattamento quando decide di esternalizzare il trattamento dei dati personali, e tale responsabile del trattamento deve essere scelto in base a criteri di competenza e alle garanzie in merito alle misure tecniche ed organizzative applicabili ai trattamenti. In presenza di un Responsabile del Trattamento, questi ha la medesima responsabilità circa la nomina di Amministratori di Sistema che trattano dati personali per conto della ASL di Pescara. Il Responsabile del trattamento è tenuto ad adottare gli adempimenti relativi alla nomina di AdS e a comunicare al Titolare del trattamento, alla UOC Sistemi Informativi, al DPO e all'Ufficio Privacy, per il tramite dei responsabili della UOC/Dipartimento in cui è in uso il sistema, l'elenco degli AdS nominati. Laddove il Responsabile del trattamento si avvalga di eventuali sub-fornitori, fermo restando l'obbligo di nomina a sub-responsabile al trattamento dei dati personali per conto della ASL di Pescara, si applica tutto quanto riportato nel presente Regolamento.
Soggetti Autorizzati al Trattamento con Delega	1) (Solo per Delegati della UOC Sistemi Informativi, della UOC Servizi Tecnici e Manutentivi e della UOC Ingegneria Clinica) Il Delegato si impegna a conformarsi al Provvedimento generale del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", così come modificato dal Provvedimento del Garante del 25 giugno 2009, e ad ogni altro pertinente provvedimento dell'Autorità. 2) In riferimento ai sistemi informatici di trattamento dei dati del Titolare, per i quali Soggetti Autorizzati alle dipendenze del Delegato esercitino attività di Amministrazione di Sistema, il Delegato si impegna a: a) designare quali amministratori di sistema le figure professionali dedicate alla gestione e alla manutenzione di impianti di elaborazione o di loro componenti con cui vengono effettuati trattamenti di Dati personali, fornendo al Titolare e al Responsabile della Protezione dei Dati, su richiesta, informazioni sulle valutazioni effettuate per le designazioni; b) effettuare un'elencazione analitica degli ambiti di operatività consentiti a ciascuno in base al relativo profilo di autorizzazione assegnato e fornendo, su richiesta, informazioni relative alle valutazioni alla base delle designazioni;

	c) predisporre e conservare l'elenco contenente gli estremi identificativi delle persone fisiche qualificate quali amministratori di sistema e le funzioni ad essi attribuite; d) comunicare periodicamente al Titolare e al Responsabile della Protezione dei Dati l'elenco aggiornato degli amministratori di sistema, specificandone l'ambito di responsabilità (sistemi, database, reti, applicativi, etc.); e) verificare annualmente l'operato degli amministratori di sistema, informando il Titolare e il Responsabile della Protezione dei Dati circa le risultanze di tale verifica; f) mantenere i file di log in conformità a quanto previsto nel suddetto provvedimento; g) garantire una rigida separazione tra chi autorizza e/o assegna i privilegi di accesso e chi effettua le attività tecnico-sistemistiche. 3) In riferimento ai sistemi informatici di trattamento dei dati del Titolare, per i quali Soggetti Esterni (previamente nominati Responsabili del Trattamento dal Delegato) esercitino attività di Amministrazione di Sistema, il Delegato si impegna a chiedere al Responsabile l'elenco degli Amministratori di Sistema ed il rispetto dei punti da a) a g) del precedente capoverso (par. 2) mediante opportuna comunicazione periodica scritta che dovrà essere tempestivamente aggiornata e comunicata ad ogni variazione di tale elenco.
Direttore della UOC Sistemi Informativi	Il Direttore della U.O.C. Sistemi Informativi ha la responsabilità di mantenere, conservare e aggiornare dell'elenco delle nomine/revoche degli Amministratori di Sistema interni alla propria Unità, così come quelle esterne relative agli Amministratori di Sistema nominati dai fornitori per i sistemi di propria competenza;
DPO	Il DPO è incaricato dei seguenti compiti: • informare e fornire consulenza al Titolare del trattamento in merito agli obblighi derivanti dal Regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati; • sorvegliare l'osservanza del regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; • fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento; • cooperare con l'Autorità di controllo; • fungere da punto di contatto per l'Autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione; • considerare debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.
Amministratori di Sistema	Gli Amministratori di sistema, a seguito della nomina sono tenuti a: • Osservare le misure di sicurezza adottate dal Titolare/Responsabile del trattamento, nonché le istruzioni tecniche dallo stesso impartite, al fine di salvaguardare la riservatezza, l'integrità e la completezza dei dati oggetto di trattamento e a ridurre i rischi di accesso non autorizzato, perdita accidentale e trattamento non consentito dei dati. • Collaborare attivamente con il Titolare/Responsabile del trattamento per verificare costantemente che siano adottate misure di sicurezza adeguate al trattamento dei dati personali.

4 Designazione e nomina

In questo articolo sono riportate le modalità di nomina ad Amministratore di Sistema per il personale interno ed esterno alla ASL di Pescara. Inoltre, vengono riportati i requisiti di attuazione delle prescrizioni contenute nel Provvedimento del 23/11/2008, relativamente ai criteri di nomina e alle modalità di gestione e verifica.

4.1 Nomina del personale interno

Su indicazione dei soggetti responsabili, dei dirigenti e/o Direttori dei Dipartimenti e delle Unità Operative Complesse, USD, UOS interessate, l'ASL di Pescara procederà alla nomina degli Amministratori di Sistema con atto protocollato sottoscritto dal SATD (Soggetto Autorizzato al Trattamento con Delega) in caso di ADS con funzione di SAT o dalla Direzione Generale in caso di ADS con funzione di SATD e, per accettazione, dall'Amministratore di Sistema nominato. Nello stesso atto di nomina quale Amministratore di Sistema l'ASL di Pescara, ai sensi degli artt. 4 comma 1 h) e 30 del Codice in materia di protezione dei dati personali (D.Lgs.196/2003 e s.m.i.), nominerà l'Amministratore di Sistema quale soggetto incaricato del trattamento dei dati, includendo una elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato, secondo i moduli allegati al presente Regolamento (sez.6).

4.2 Nomina del personale esterno

Il Provvedimento del Garante prevede che le società fornitrici di servizi di cui alla Sez. 2 debbano provvedere al loro interno alla nomina degli Amministratori di Sistema. Pertanto, la ASL di Pescara, all'avvio di un rapporto di fornitura, dovrà designare le aziende fornitrici quali Responsabili dei trattamenti di dati personali, rispetto ai quali sono chiamate a svolgere funzioni di Amministratore di Sistema. La normativa vigente prevede che debba essere il Responsabile del Trattamento, dunque la società che fornisce il servizio, a provvedere alla nomina dell'Amministratore di Sistema (v. Sez. 3.3 "Ruoli").

Le nomine dei soggetti esterni devono obbligatoriamente contenere l'elenco completo ed esaustivo delle funzioni, dei compiti e di tutte le facoltà e i privilegi tecnici, organizzativi ed operativi che spettano a ciascun Amministratore. Nel caso di coesistenza, per un dato sistema, di AdS interni ed esterni, deve essere distinto l'ambito di responsabilità dei singoli ADS.

4.3 Valutazione delle caratteristiche soggettive

Precedentemente al conferimento dell'incarico, il soggetto nominante si impegna a valutare attentamente:

1. le caratteristiche soggettive della persona designata in termini di esperienza, competenza e affidabilità;
2. la partecipazione del soggetto ai percorsi di formazione previsti;
3. eventuali e comprovati vincoli di naturale organizzativa e personale che possano impedire al soggetto lo svolgimento dell'incarico;
4. il corretto bilanciamento dei carichi di lavoro dovuti alle normali mansioni quotidiane o all'accumulo di più ruoli da AdS su sistemi differenti;
5. un'equa distribuzione degli incarichi all'interno dei gruppi di lavoro.

Ai soggetti interni designati è sempre richiesta la presa visione, la comprensione e l'accettazione delle disposizioni vigenti in materia di trattamento dei dati personali e delle norme di sicurezza, con particolare riferimento a:

- Conoscenza delle normative di leggi applicabili;
- Conoscenza delle politiche interne alla struttura sanitaria;
- Riferimento in materia di gestione sicura dei sistemi informatici;
- Consapevolezza dei rischi di sicurezza derivanti da errori, omissioni e violazioni delle regole applicabili allo svolgimento delle attività di Amministratore di sistema;

- Conoscenza e consapevolezza di eventuali limitazioni o vincoli di qualsiasi natura che possano impedire il corretto svolgimento delle funzioni di AdS per il sistema di fattispecie.

Per quanto riguarda gli Amministratori di Sistema in forza presso fornitori esterni, il processo di valutazione delle caratteristiche soggettive si intende e a carico della società fornitrice del servizio. I requisiti degli ADS definiti nella presente politica devono essere inclusi nelle clausole contrattuali che normano il conferimento del ruolo di Responsabile del trattamento. Tali valutazioni possono in ogni momento essere verificate e validate dal Titolare del trattamento o da persone interne incaricate dall'Azienda.

4.4 Designazione individuale

L'attribuzione dell'incarico di Amministratore di Sistema deve essere individuale, ovvero la persona designata deve essere identificabile in maniera univoca. A tale scopo l'Azienda, nella persona del soggetto nominante, predispone una specifica lettera di incarico (v. modello Allegato Sez. 6) contenente almeno le seguenti informazioni:

- elencazione analitica degli ambiti di operatività richiesti e consentiti, in base al profilo di autorizzazione assegnato;
- notifica che l'operato dell'Amministratore di Sistema può essere soggetto a verifiche con cadenza perlomeno annuale, anche attraverso la rilevazione e la successiva analisi dei log di accesso (login, logout) generati nel corso dello svolgimento delle attività di amministrazione;
- notifica che la nomina ed il relativo nominativo potrebbero essere comunicati al personale ed eventualmente a terzi ove e nei modi previsti dalle vigenti leggi;

La lettera di nomina ad Amministratore di Sistema deve essere firmata, in duplice originale, per accettazione dalla persona designata, e opportunamente conservata da parte delle funzioni competenti individuate nell'ambito dell'Azienda (v. Sez. 3.3 "Ruoli").

4.5 Gestione delle credenziali

In linea generale, limitatamente ai vincoli tecnologici, viene adottato un sistema di credenziali assegnate indivdualmente, e non condivise, per tutti gli accessi ai sistemi e alle risorse amministrate. Le credenziali di accesso privilegiato, incluse quelle ad esempio degli utenti "root" e "administrator", devono essere gestite con la massima cura e, salvo comprovati vincoli e limitazioni, non divulgate né utilizzate in maniera impropria. Quelle di default, ove possibile, vanno disattivate e/o modificate tempestivamente. La custodia delle password deve avvenire con metodologie sicure (es. password manager, gestione centralizzata) e soggetta a politiche di complessità e rotazione regolari. Le credenziali assegnate devono garantire permessi e privilegi sufficienti a poter espletare tutte le funzioni previste dal ruolo di AdS.

Resta inteso che il soggetto nominante (es. SATD), all'atto della nomina dell'AdS, si impegna a fornire tempestivamente tutte le risorse informative e tecniche necessarie alla presa in carico del sistema, compresi i contatti con eventuali soggetti esterni e/o interni.

4.6 Gestione dell'elenco degli Amministratori di Sistema

Con il presente Regolamento si prescrive la creazione di un elenco degli Amministratori di Sistema che deve contenere, come minimo, le seguenti informazioni:

- gli estremi identificativi delle persone fisiche designate, la cui attività riguarda anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di dati personali;
- l'elenco delle mansioni operative e del ruolo ad essi attribuito.

L'elenco contenente gli estremi identificativi dei dipendenti designati come Amministratori di Sistema e l'ambito di operatività ad essi attribuito deve essere mantenuto aggiornato e disponibile in caso di accertamenti da parte del Garante. La revisione di correttezza delle informazioni indicate nell'elenco deve essere eseguita almeno una volta l'anno, fermo restando che eventuali aggiornamenti in caso di nuove nomine o revoche degli incarichi devono essere prontamente riportati a cura delle Unità Operative competenti.

La designazione e la gestione degli elenchi di eventuali Amministratori corrispondenti a collaboratori esterni operanti presso l'Azienda vengono demandati alle relative società fornitrici. Tali elenchi dovranno essere redatti e comunicati, al verificarsi delle seguenti condizioni:

- all'avvio del contratto di fornitura;
- ad ogni aggiornamento derivante dalla sostituzione di operatori;
- ad ogni richiesta da parte del Titolare del trattamento o persone da questi designate
- alla cessazione dell'incarico del personale addetto

La designazione dell'AdS, sia esterno che interno all'organizzazione del Titolare, dovrà essere inserita nel Registro dei trattamenti, previa richiesta formale all'ufficio privacy, ad opera del SATD competente.

L'elenco degli AdS viene reso disponibile in caso di richiesta da parte dell'Autorità Garante, nei casi previsti per legge.

5 Verifica e controllo

5.1 Registrazione degli accessi (log)

Il Provvedimento del Garante richiede la registrazione degli accessi logici ai sistemi da parte degli Amministratori. In particolare, la normativa distingue le tipologie di "access log" e "event records", con le seguenti definizioni:

- **Access Log**: Per access log si intende la registrazione degli eventi generati dal sistema di autenticazione informatica all'atto dell'accesso o tentativo di accesso da parte di un Amministratore di Sistema o all'atto della sua disconnessione.
- **Event records:** Gli event records generati dai sistemi di autenticazione contengono usualmente i seguenti riferimenti: nome utente (username) utilizzato; data e ora dell'evento (timestamp); descrizione dell'evento contenente informazioni aggiuntive come il sistema di elaborazione o software utilizzato, se si tratta di accesso (login) o disconnessione (logout), eventuali errori, linea di comunicazione o dispositivo utilizzato, ecc.

La norma prescrive che i log mantenuti presentino caratteristiche di completezza, inalterabilità e integrità.
La caratteristica di **completezza** si riferisce all'insieme degli eventi censiti nel sistema di log, che deve comprendere tutti gli eventi di accesso generati dalle attività degli Amministratori di Sistema su tutti i sistemi di elaborazione (server, client, database) con cui vengono trattati, anche indirettamente, dati personali. Le

registrazioni devono inoltre comprendere, i riferimenti temporali e la descrizione dell'evento che le ha generate.
Le caratteristiche legate all'**inalterabilità** dei dati raccolti dai sistemi di log, viene soddisfatta ad esempio, attraverso l'implementazione di una piattaforma centralizzata per la gestione dei log con l'utilizzo di canali di trasmissione sicuri o l'utilizzo di supporti non riscrivibili per la conservazione dei log.
La caratteristica legata alla possibilità di verifica dell'**integrità** dei log viene soddisfatta, ad esempio, tramite l'applicazione di tecniche di cifratura, timestamping o hashing.
Pertanto, sono implementate idonee soluzioni tecnologiche atte a garantire la creazione e la raccolta dei log di accesso degli Amministratori di Sistema, secondo le caratteristiche appena riportate.
I log di accesso ai sistemi di elaborazione e agli archivi elettronici effettuati dagli Amministratori di Sistema sono conservati per un congruo periodo, non inferiore a 6 mesi. Trascorso tale periodo, dovrà esserne prevista la cancellazione definitiva da ogni supporto di archiviazione.
Rientrano nell'obbligo di registrazione degli accessi sia i sistemi server che i sistemi client, definiti come *postazioni di lavoro informatizzate*.
Come specificato dal Garante nelle risposte alle domande più frequenti (FAQ) del Provvedimento "Amministratori di sistema" del 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008), nei casi più semplici, il requisito di mantenimento dei log può essere soddisfatto tramite funzionalità già disponibili nei più diffusi sistemi operativi, senza richiedere necessariamente l'uso di strumenti software o hardware aggiuntivi. Per esempio, la registrazione locale dei dati di accesso su una postazione, in determinati contesti, può essere ritenuta idonea al corretto adempimento qualora goda di sufficienti garanzie di integrità.
Resta in carico al Titolare ogni valutazione relativa all'idoneità degli strumenti disponibili oppure l'adozione di strumenti più sofisticati, quali la raccolta dei log centralizzata e l'utilizzo di dispositivi non riscrivibili o di tecniche crittografiche per la verifica dell'integrità delle registrazioni.

5.2 Verifiche periodiche

Sono disposte verifiche periodiche sull'operato degli Amministratori di Sistema con cadenza almeno annuale, per rilevarne la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali. Di seguito sono descritte le attività di verifica, con una indicazione di massima sulla rispettiva cadenza periodica:

Cadenza annuale:

- verifiche di riscontro, su un campione significativo di sistemi, della corretta generazione dei log di accesso, della loro conformità e della conservazione sicura degli stessi per almeno sei mesi;
- analisi di dettaglio dei log di accesso, al fine di riscontrare eventuali anomalie nella frequenza degli accessi e nelle loro modalità (orari, durata, sistemi cui si è fatto accesso, postazioni di lavoro utilizzate, ecc …);
- verifiche di riscontro dell'attuazione del processo di gestione dell'elenco degli Amministratori di Sistema e verifica dell'allineamento di tale lista, con l'assegnazione dei ruoli e dei relativi ambiti di operatività, comprese le credenziali applicative;
- i SATD e gli altri soggetti responsabili provvederanno a trasmettere al Titolare del trattamento, all'Ufficio Privacy e Sicurezza delle Informazioni, al DPO e al Direttore Sistemi Informativi, i report denominati "Rapporto di verifica delle attività svolte dagli Amministratori di sistema";
- verifica della permanenza delle caratteristiche soggettive valutate in fase di nomina (v. sez. 4.3).

Su richiesta:

- ogni qualvolta ve ne sia necessità interna (anche da parte dell'AdS stesso) o su richiesta degli organi esterni (es. Autorità Giudiziaria, Garante) per attività di controllo specifiche. Le suddette attività di verifica dovranno essere documentate tramite la redazione di un report denominato "Rapporto di verifica delle attività svolte dagli Amministratori di sistema", attestante:
  - la data di esecuzione delle attività;
  - l'ambito di applicazione (scope) delle verifiche effettuate (es. sistemi interessati, tipologie di log, ecc.);
  - i componenti del team di verifica ed eventuali altre figure presenti;
  - le tipologie di verifiche compiute ed i relativi esiti;
  - le eventuali non conformità o anomalie rilevate;
  - gli eventuali piani di azione e mitigazione a fronte delle non conformità rilevate al punto precedente, con la chiara indicazione di:
    - Ruoli e responsabilità per l'esecuzione e la verifica delle attività previste;
    - Modalità e tempistiche dell'applicazione dei piani di azione e mitigazione.

6 Allegati

6.1 All. 1: Modello di nomina ad Amministratore di Sistema per il personale dipendente

INCARICO DI AMMINISTRATORE DI SISTEMA

ADDENDUM ALL'AUTORIZZAZIONE AL TRATTAMENTO

ai sensi dell'art. 2-quaterdecies del D.Lgs. 196/03 e dell'art. 29 del Regolamento UE 2016/679

Prot. n. Pescara, lì

Sig./Sig.ra _____

Ruolo: _____

Posta Elettronica _____

L'ASL di Pescara incarica del ruolo di amministratore di sistema il

Sig./Sig.ra:

codice fiscale:

lavoratore dell'organizzazione:

nei seguenti termini e condizioni

a) Il Regolamento UE 2016/679, in particolare agli articoli 5 e 24, pone con forza l'accento sulla "responsabilizzazione" (accountability) di titolari e responsabili – ossia, sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento;
b) rientra nel concetto di "accountability" anche l'individuazione di figure professionali dedicate alla programmazione, cura, gestione e manutenzione di strumenti, impianti e apparecchi destinati alla elaborazione con cui vengano

effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise resource planning), le reti locali e gli apparati di sicurezza.

c) Il Garante per la protezione dei dati personali ha adottato il provvedimento del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008);
d) ai sensi e per gli effetti di cui all'articolo 22, comma 4, del decreto legislativo n.101 del 10/8//2018, il provvedimento del Garante per la protezione dei dati personali del 27/11/2008 è da ritenersi compatibile con il regolamento Ue 2016/679 e con il citato decreto legislativo;
e) l'amministratore di sistema qui incaricato possiede i requisiti di esperienza, capacità e affidabilità, fornendo idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza (all. 1 Curriculum)
f) Le parti danno atto che il Titolare del Trattamento predispone e gestisce sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte di tutte le persone qualificate amministratori di sistema.
g) Il Titolare del Trattamento provvede, altresì, con cadenza almeno annuale, a svolgere le dovute verifiche sulle attività compiute dall'Amministratore di sistema. È obbligo di quest'ultimo prestare alla Società la sua piena collaborazione per il compimento delle verifiche stesse; in ogni caso, è tenuto a predisporre, con cadenza trimestrale (o altra cadenza), una relazione scritta delle attività svolte in esecuzione delle incombenze affidatigli in forza del presente atto.
h) Con separati atti vengono inoltre assegnati all'Amministratore di sistema i necessari poteri e supporti economici ed organizzativi per l'adeguamento di tutte le misure di sicurezza, come previsto dalle vigenti disposizioni in materia di sicurezza del trattamento dei dati.
i) Della nomina ad Amministratore di sistema, così disposta con il presente atto, verrà data opportuna informazione nell'ambito dell'organizzazione aziendale della Società, ed al personale interessato

al quale sono affidati i seguenti compiti

(indicare in maniera analitica le incombenze dell'amministratore di sistema; la seguente elencazione è meramente esemplificativa – cancellare ipotesi che non ricorrono – aggiungere ipotesi non formulate)

j) gestire il sistema informativo in osservanza alle norme legislative e regolamentari nonché attenendosi anche alle disposizioni del Titolare in tema di sicurezza disposte mediante analisi dei rischi, DPIA (Data protection impact assessment), policies interne;
k) predisporre ed aggiornare un sistema di sicurezza idoneo a rispettare le prescrizioni dell'art. 32 Regolamento UE 2016/679, adeguandolo anche alle eventuali future norme in materia di sicurezza;
l) amministrare le misure tecniche e organizzative adottate al fine di garantire un livello di sicurezza adeguato al rischio, idoneo, in particolare, a conseguire:
    a. la pseudonimizzazione e la cifratura dei dati personali;
    b. la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, tenendo conto delle minacce potenzialmente derivanti sia da eventi naturali che da azioni dolose di terzi e garantendo alta affidabilità, Disaster Recovery e Business Continuity;
    c. la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
m) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento, verificando sia i singoli componenti che l'intero sistema (ivi inclusi gli elementi ridondanti, se presenti);
n) sovraintendere agli accessi ai sistemi informativi ed agli elaboratori e a qualunque dispositivo e, conseguentemente, assegnare e amministrare il sistema delle credenziali di autenticazione, compresa la disabilitazione in relazione a eventi quali venir meno delle qualità sottese alla precedente abilitazione, inerzia dell'utilizzatore per un periodo minimo significativo predefinito,
o) adottare adeguati programmi antintrusione, antivirus, firewall ed altri strumenti software o hardware atti a garantire la massima misura di sicurezza nel rispetto di quanto dettato dal GDPR e dalle altre norme in materia ed utilizzando le conoscenze acquisite in base al progresso tecnico software e hardware, verificandone l'installazione, l'aggiornamento ed il funzionamento degli stessi;
p) adottare, sulla base della pianificazione approvata dal titolare del trattamento e, comunque, sempre in caso di situazioni di urgenza e di emergenza, tutti i provvedimenti e gli accorgimenti, tecnici e organizzativi, necessari ad

evitare la modifica, la perdita o la distruzione, accidentale o dolosa, dei dati personali e provvedere al ricovero periodico degli stessi con copie di back-up, vigilando sulle relative procedure. L'Amministratore di sistema dovrà anche assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro;

q) provvedere direttamente o per il tramite di idoneo outsourcer alla distruzione e smaltimento di elaboratori e supporti di memorizzazione di qualunque natura e/o alla cancellazione dei dati prodromica al reimpiego di elaboratori e supporti, nell'osservanza delle norme di legge e del Provvedimento del Garante per la Protezione dei Dati personali del 13 ottobre 2008 in materia di "Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali" (pubblicato sulla G.U. n. 287 del 9 dicembre 2008);

r) cooperare nella predisposizione del documento di Analisi dei Rischio e della DPIA per la parte concernente il sistema informatico ed il trattamento informatico dei dati;

s) istituire e tenere il registro delle violazioni ex art. 33 GDPR ult. par., nonché effettuare accurate indagini e istruttorie a riguardo dei casi di data breach (art. 34 GDPR), procedendo alle notificazioni e alle comunicazioni agli interessati (artt. 34 e 35 GDPR), di concerto con il titolare del trattamento e, se costituito, con il Team di Rischio;

t) coordinare, di concerto con il Titolare del Trattamento, le attività esecutive degli autorizzati al trattamento nello svolgimento delle mansioni loro affidate per garantire un corretto, lecito e sicuro trattamento dei dati personali;

u) collaborare con il Titolare del Trattamento per l'attuazione delle prescrizioni impartite dal Garante;

v) comunicare prontamente al Titolare del Trattamento qualsiasi situazione che possa compromettere il corretto trattamento dei dati personali.

ID	Nome del sistema	Descrizione del sistema	Funzioni dell'ADS
1			
2			
3			
4			
5			
6			
7			
8			
Ultimo aggiornamento dell'elenco		_____ /_____ /_____	

Per quanto non disposto dalla presente scrittura, le parti rinviano a quanto previsto dalle norme europee e nazionali rilevanti in materia di protezione dei dati personali nonché dalle linee guida, dalle raccomandazioni e dalle best practices adottate dal Comitato Europeo per la Protezione dei Dati o da altre autorità di controllo e di settore competenti.

Luogo/data .....

IL TITOLARE DEL TRATTAMENTO

(Il Legale Rappresentante)

.....

Sottoscrive per presa visione e accettazione

L'AMMINISTRATORE DI SISTEMA

.....

Politica aziendale di gestione degli incidenti informatici

Revisioni Documento

Classificazione	**RISERVATO – Uso interno**
Redazione	**M. D'Alessandro**
Verifica	**Direttore UOC Sistemi Informativi**
Approvazione	**Titolare del trattamento**

Storico revisioni

Versione	**Data**	**Autore**	**Note**
1.0.0	01/03/2026	M. D'Alessandro	Prima redazione
1.0.1	14/07/2026	DPO, M. D'Angelo	Revisione e modifiche per conformità a GDPR e coinvolgimento del DPO
1.1	29/07/2026	M. D'Alessandro	Emissione

Lista di distribuzione

Destinatario	**Motivo**
Direttore Generale	Per competenza
Direttore Sanitario aziendale	
Direttore Amministrativo aziendale	
Ufficio Privacy e Sicurezza delle Informazioni	
Ai Soggetti Autorizzati al Trattamento con delega (SATD)	

Sommario

1. Scopo e campo di applicazione

1.1 Scopo

La presente Politica definisce le modalità di gestione degli incidenti di sicurezza informatica adottate dalla ASL di Pescara e ne stabilisce i principi, le responsabilità, i criteri di classificazione e gli obblighi di notifica in conformità al D.Lgs. 4 settembre 2024, n. 138, che recepisce la Direttiva (UE) 2022/2555 (NIS2).

La Politica persegue i seguenti obiettivi:

- Definire un approccio strutturato, tempestivo e proporzionato alla gestione degli incidenti di sicurezza informatica;
- Garantire la continuità dell'erogazione dei servizi sanitari essenziali anche in caso di incidente;
- Assicurare il rispetto degli obblighi di notifica all'ACN/CSIRT Italia (Art. 25 D.Lgs. 138/2024) e al Garante Privacy (Art. 33 GDPR);
- Definire ruoli, responsabilità e catena di escalation per la risposta agli incidenti;
- Promuovere il miglioramento continuo attraverso l'analisi post-incidente;
- Ridurre l'esposizione al rischio cyber, in particolare per i sistemi critici.

1.2 Campo di applicazione

La presente politica si applica a:

- Tutti i sistemi informativi e di rete dell'ASL, inclusi (elenco non esaustivo):
  - i sistemi clinici (HIS, LIS, RIS/PACS, CUP, sistema farmaceutico, sistemi DEA/PS);
  - l'infrastruttura ICT (server, endpoint, rete, cloud)
  - i dispositivi medici connessi (IoMT).
- Tutto il personale dell'ASL, inclusi dipendenti, collaboratori, personale sanitario;
- Tutti i fornitori, partner e terze parti che accedono o gestiscono sistemi informativi dell'ASL;
- Tutti i servizi erogati dall'ASL classificati come essenziali ai sensi dell'Allegato I, D.Lgs. 138/2024 (settore Sanitario).

2. Riferimenti normativi

La presente Politica è elaborata in conformità ai seguenti riferimenti normativi e standard di settore:

Riferimento	Titolo e rilevanza
D.Lgs. 138/2024	Recepimento Direttiva NIS2 – obbligo principale. Artt. 23-24 (misure e governance), Art. 25 (notifica incidenti), Art. 38, comma 7 (responsabilità dei dipendenti pubblici) e comma 9, lett. c) (regime sanzionatorio per le PA). Soggetto Essenziale – Settore Sanità (Allegato I)
Direttiva (UE) 2022/2555	Direttiva NIS2 – fonte primaria europea
L. 90/2024	Disposizioni in materia di rafforzamento della cybersicurezza nazionale – istituzione Referente per la Cybersicurezza
GDPR – Reg. (UE) 2016/679	Art. 33: obbligo di notifica al Garante Privacy entro 72h per data breach. Coordina con gli obblighi NIS2 per doppia notifica
D.Lgs. 196/2003 s.m.i.	Codice Privacy italiano
Det. ACN 379907/2025	Misure di sicurezza di base
Det. ACN 333017/2025	Designazione Punto di Contatto
Framework Nazionale per la Cybersecurity e la Data Protection – Edizione 2025 (FNCDP v2.1)	Strumento di riferimento nazionale – Funzioni GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER
NIST CSF 2.0	Standard internazionale di riferimento
ISO/IEC 27001:2022	Sistema di gestione della sicurezza delle informazioni
ISO/IEC 27035	Gestione degli incidenti di sicurezza delle informazioni
ENISA Good Practice Guide for Incident Management	Linee guida ENISA per la gestione degli incidenti
Linee Guida ACN – Notifica Incidenti	Istruzioni operative per la notifica al portale CSIRT Italia

3. Definizioni

Termine	Definizione
Incidente di sicurezza informatica	Evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati, o dei servizi offerti dai sistemi informativi e di rete dell'ASL (Art. 2, c.1, lett. t), D.Lgs. 138/2024).
Incidente significativo	Incidente che ha causato o è in grado di causare: • una grave perturbazione operativa dei servizi o perdite finanziarie; • ripercussioni su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli (Art. 25, c.4, D.Lgs. 138/2024).
Incidente IS-1 (ACN)	Il soggetto NIS ha evidenza della perdita di riservatezza, verso l'esterno, di dati digitali di sua proprietà o sui quali esercita il controllo (es. data breach dati pazienti). Det. ACN 164179/2025, 379907/2025, All.4.
Incidente IS-2 (ACN)	Il soggetto NIS ha evidenza della perdita di integrità, con impatto verso l'esterno, di dati di sua proprietà o sui quali esercita il controllo (es. alterazione referti). Det. ACN 164179/2025, 379907/2025, All.4.
Incidente IS-3 (ACN)	Il soggetto NIS ha evidenza della violazione dei livelli di servizio attesi, sulla base degli SL definiti ai sensi della misura DE.CM-01 (es. blocco HIS per ransomware). Det. ACN 164179/2025, 379907/2025, All.4.
Incidente IS-4 (ACN)	Il soggetto NIS ha evidenza dell'accesso non autorizzato o con abuso dei privilegi concessi, a dati digitali di sua proprietà o sui quali esercita il controllo (es. accesso abusivo cartelle cliniche). Det. ACN 164179/2025, 379907/2025, All.4.
Quasi-incidente	Evento che avrebbe potuto configurare un incidente senza che quest'ultimo si sia verificato, incluso il caso in cui sia stato efficacemente evitato (es. phishing bloccato, malware isolato prima della diffusione).
Incidente non-cyber	Evento che causa interruzione o degrado dei servizi ICT senza origine cibernetica (es. guasto hardware, interruzione alimentazione). Gestito con le stesse procedure interne ma non necessariamente soggetto a notifica NIS2.
Data breach	Violazione di sicurezza che comporta accidentalmente o illecitamente la distruzione, perdita, modifica, divulgazione non autorizzata o accesso a

Termine	Definizione
	dati personali. Doppio obbligo di notifica: ACN (NIS2) e Garante Privacy (GDPR Art. 33) entro 72h.
Evidenza dell'incidente	Insieme di elementi oggettivi dai quali si evince che si è verificato un incidente di sicurezza informatica. Definisce il momento dal quale decorrono i termini di notifica all'ACN (24h per pre-notifica, 72h per notifica).
Pre-notifica (early warning)	Prima comunicazione al CSIRT Italia, entro 24h dall'acquisizione dell'evidenza dell'incidente significativo.
Notifica dell'incidente	Comunicazione completa al CSIRT Italia entro 72h, con valutazione iniziale di gravità e impatto, e indicatori di compromissione (IoC) ove disponibili.
Relazione finale	Documento trasmesso al CSIRT Italia entro 1 mese dalla notifica, con descrizione dettagliata, causa radice, misure adottate e lezioni apprese.
CSIRT Italia	Computer Security Incident Response Team italiano – unità operativa dell'ACN. Destinatario delle notifiche NIS2. Portale: https://www.csirt.gov.it/segnalazione
ACN	Agenzia per la Cybersicurezza Nazionale – Autorità nazionale competente NIS2 in Italia.
IoC	Indicator of Compromise – artefatto osservabile che indica una possibile compromissione (IP, hash malware, dominio C2, ransom note).
CSIRT Aziendale/Team di Risposta	Gruppo multidisciplinare interno dell'ASL incaricato della gestione operativa degli incidenti.
RTO / RPO	Recovery Time Objective / Recovery Point Objective – obiettivi di ripristino definiti per sistema clinico. Violazione degli SL attesi = trigger IS-3.

4. Principi generali

Sono di seguito riassunti i principi essenziali che guidano la presente politica:

Principio	Descrizione ed applicazione nel contesto aziendale
Continuità delle cure	La gestione degli incidenti deve prioritizzare la continuità dell'assistenza sanitaria. Un incidente che compromette sistemi clinici critici può mettere a rischio la vita dei pazienti. La risposta tecnica non può prescindere dall'attivazione delle procedure di fallback clinico.
Proporzionalità	La risposta agli incidenti è commisurata alla gravità, all'impatto clinico e alla complessità dell'evento. Le risorse impiegate sono proporzionate alla classificazione P1-P4 e alla tipologia IS-1÷IS-4.
Tempestività	Gli incidenti devono essere gestiti con la massima urgenza. I termini NIS2 (24h pre-notifica, 72h notifica) decorrono dall'acquisizione dell'evidenza. Il dubbio sulla significatività non sospende l'obbligo: meglio notificare in eccesso che in difetto.
Trasparenza	Le informazioni sugli incidenti devono essere condivise tempestivamente con gli attori appropriati (direzione strategica, apparato dirigenziale, personale sanitario, ACN, Garante, pazienti ove necessario), nel rispetto della riservatezza e delle normative vigenti.
Doppia notifica	In caso di incidente che coinvolga dati personali di pazienti (data breach), l'Azienda è soggetta al doppio obbligo di notifica: ACN/CSIRT Italia (NIS2) e Garante Privacy (GDPR). I due processi sono paralleli e non si sostituiscono.
Responsabilità personale	Il Direttore Generale risponde personalmente degli obblighi NIS2 (Art. 38 comma 7 D.Lgs. 138/2024). La delega operativa al Referente per la Cybersicurezza non esonera il management dalla supervisione.
Miglioramento continuo	Ogni incidente è un'opportunità di apprendimento. La Root Cause Analysis obbligatoria e le Lessons Learned alimentano il Risk Register ASL, aggiornano le procedure e rafforzano le misure preventive.
Documentazione integrale	Ogni incidente, inclusi i quasi-incidenti, deve essere formalmente segnalato, analizzato e documentato nel Registro degli Incidenti. La documentazione è fondamentale per audit, ispezioni ACN e procedimenti legali.

5. Ruoli e responsabilità

5.1 Struttura di governance degli incidenti

La gestione degli incidenti di sicurezza informatica è articolata su due livelli:

- il Team di Gestione degli Incidenti (TGI), organo decisionale;
- il Team Operativo (CSIRT Aziendale), organo esecutivo.

Solo i soggetti interni all'ASL sono deputati a determinare la configurazione di un incidente, la sua gravità e le azioni da intraprendere.

5.1.1 Team di gestione degli incidenti (TGI) – Organo decisionale

Il TGI è istituito e operante a prescindere dal verificarsi di un incidente. Si riunisce entro 72 ore dalla ricezione di una segnalazione di potenziale incidente significativo. La composizione è la seguente:

Figura	Ruolo nel TGI	Responsabilità specifiche NIS2/L.90/2024
Direttore Generale (DG)	Management body ex Art. 23 D.Lgs. 138/2024 – presiede il TGI per incidenti P1	Approvazione misure di gestione del rischio; supervisione attuazione; responsabilità personale Art. 38, comma 7; autorizzazione dichiarazione emergenza operativa
Direttore Amministrativo (DA)	Management body ex Art. 23 D.Lgs. 138/2024	Gestione implicazioni economiche e legali; approvazione comunicazioni esterne; coordinamento con assicurazione cyber
Direttore Sanitario (DS)	Management body ex Art. 20 D.Lgs. 138/2024	Attivazione procedure di fallback clinico; coordinamento con reparti; comunicazione ai pazienti; gestione impatto su sicurezza delle cure
Referente per la Cybersicurezza Aziendale (L.90/2024)	CISO de facto – coordinatore operativo del TGI	Coordinamento risposta tecnica; supervisione CSIRT Aziendale; reporting alla DG; interfaccia con ACN; aggiornamento Risk Register
Punto di Contatto NIS2	Interfaccia formale con ACN ex D.Lgs. 138/2024	Interlocuzione ufficiale con ACN; firma notifiche NIS2; aggiornamento registrazione portale ACN
Sostituto Punto di Contatto NIS2	Interfaccia formale con ACN ex D.Lgs. 138/2024	Sostituisce il Punto di Contatto in sua assenza; stesse funzioni tranne la registrazione iniziale

Figura	Ruolo nel TGI	Responsabilità specifiche NIS2/L.90/2024
Referente CSIRT	Responsabile operativo notifiche CSIRT Italia	Trasmissione pre-notifica e notifica tramite portale CSIRT Italia; redazione relazioni intermedie e finale; coordinamento con CSIRT Italia
DPO e Ufficio Privacy	Valutazione profili di impatto sui dati personali ai sensi del GDPR	Valuta se l'incidente costituisce data breach; coordina notifica al Garante Privacy; parere su comunicazione agli interessati

Alle riunioni del TGI possono partecipare in veste consultiva, senza potere decisionale:

- Fornitori o attori esterni coinvolti nell'incidente;
- SOC esterno;
- Consulenti legali;
- Direttori delle UO Operative interessate, ove del caso:
  - UOC Ingegneria Clinica;
  - UOC Servizi Tecnici e Manutentivi;
  - UOSD Progettazioni e Nuove Realizzazioni;
  - Direttori di UOC e Responsabili di UOSD;
  - UOC Acquisizione Beni e Servizi;
  - UOC Dinamiche del Personale;
  - UOS Formazione e Ricerca;
  - UOS Risk Management.

I verbali di ogni riunione devono essere documentati e conservati per almeno 5 anni.

5.1.2 CSIRT Aziendale - Team tecnico-operativo

Il CSIRT Aziendale gestisce operativamente la risposta tecnica agli incidenti. È composto da:

- Responsabile del CSIRT Aziendale: Referente per la Cybersicurezza Aziendale (L.90/2024)
- Direttore UOC Sistemi Informativi: responsabile dell'implementazione tecnica delle misure di contenimento e ripristino
- Personale ICT specializzato (sicurezza, sistemisti, DBA) con accesso ai sistemi coinvolti, interno (UOC Sistemi Informativi o personale tecnico informatico incardinato in altre UO) o esterno (SOC, fornitori o consulenti specalizzati)
- Referente CSIRT: interfaccia con CSIRT Italia

5.2 Responsabilità di tutto il personale

Tutto il personale della ASL di Pescara, operante a qualunque titolo e con qualunque mansione, anche non tecnica, ha l'obbligo di:

- Segnalare tempestivamente al CSIRT Aziendale qualsiasi anomalia osservata sui sistemi informatici;
- Non spegnere, formattare o modificare i sistemi potenzialmente compromessi prima del nulla osta del CSIRT Aziendale;
- Non divulgare informazioni sull'incidente a persone non autorizzate;
- Cooperare con il CSIRT Aziendale fornendo tutte le informazioni richieste;
- Attivare le procedure di fallback clinico (cartacee) comunicate dalla Direzione Sanitaria per garantire la continuità delle cure in via prioritaria.

5.3 Responsabilità dei fornitori e del personale esterno

I fornitori e le terze parti operanti a qualunque titolo presso la ASL di Pescara, aventi accesso ai sistemi aziendali, hanno l'obbligo di:

- Notificare immediatamente all’azienda qualsiasi incidente che coinvolga sistemi o dati ASL, come da clausole contrattuali NIS2;
- Cooperare pienamente con il CSIRT Aziendale nelle attività di analisi, contenimento e ripristino;
- Non intraprendere azioni di remediation che possano distruggere evidenze forensi senza autorizzazione del CSIRT Aziendale.

6. Classificazione degli incidenti

6.1 Schema di classificazione

La classificazione degli incidenti dell'ASL impiega uno schema ibrido, che integra le tipologie di incidenti significativi definite previste dall'ACN (IS-1÷IS-4, Det. ACN 379907/2025, All.4.) con una scala di priorità operativa interna (P1÷P4), che tiene conto dell'impatto clinico specifico del contesto sanitario.

6.1.1 Tipologie di Incidenti Significativi NIS2 (ACN – Det. 379907/2025)

Un incidente è classificato come significativo ai sensi NIS2 quando l'ASL ha evidenza oggettiva di uno dei seguenti scenari. La classificazione come IS attiva l'obbligo di notifica al CSIRT Italia:

Tipo	Categoria	Descrizione (Det. ACN 164179/2025)	Esempi nel contesto ASL di Pescara
IS-1	**Perdita di Riservatezza**	Il soggetto NIS ha evidenza della perdita di riservatezza, verso l'esterno, di dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale.	Data breach dati sanitari pazienti; diffusione non autorizzata cartelle cliniche; esfiltrazione dati da HIS/LIS; pubblicazione online di dati ASL
IS-2	**Perdita di Integrità**	Il soggetto NIS ha evidenza della perdita di integrità, con impatto verso l'esterno, di dati di sua proprietà o sui quali esercita il controllo, anche parziale.	Alterazione referti di laboratorio; manipolazione dati terapeutici in HIS; modifica non autorizzata di risultati diagnostici con impatto esterno
IS-3	**Violazione Livelli di Servizio**	Il soggetto NIS ha evidenza della violazione dei livelli di servizio attesi, sulla base degli SL definiti ai sensi della misura DE.CM-01.	Ransomware che blocca i servizi critici oltre i livelli di servizio attesi; Blocco prolungato su CUP oltre i livelli di servizio attesi; indisponibilità fascicolo sanitario elettronico (FSE)
IS-4	**Accesso Non Autorizzato**	Il soggetto NIS ha evidenza dell'accesso non autorizzato o con abuso dei privilegi concessi, a dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale.	Accesso abusivo a cartelle cliniche; uso di credenziali rubate per accedere a sistemi critici; amministratore di sistema che accede a dati fuori dalla propria mansione

6.1.2 Scala di priorità operativa interna (P1 ÷ P4)

La scala di priorità operativa definisce il livello di urgenza della risposta e la catena di escalation. È determinata congiuntamente dal Referente per la Cybersicurezza e dal Direttore della UOC Sistemi Informativi sulla base dell'impatto clinico e ICT:

P	Livello	Trigger Clinico (impatto su cure)	Trigger ICT (impatto informatico)	Azioni immediate e Notifica NIS2 (esempi)
P1	**CRITICO**	Blocco DEA/PS; interruzione terapie salvavita; deviazione ambulanze; impossibilità accesso dati paziente in emergenza	Ransomware attivo su HIS/AD; rete ospedaliera down; backup cifrati; esfiltrazione dati in corso	Attivazione CSIRT Aziendale immediata. DG informato entro 30 min. Fallback clinico attivato. Pre-notifica ACN obbligatoria entro 24h. Valutazione data breach per Garante.
P2	**ALTO**	Blocco CUP; interruzione LIS urgenze; blocco farmaceutica; indisponibilità PACS; degradazione HIS	Malware con movimento laterale; compromissione account privilegiato; blocco applicativo clinico; accesso non autorizzato HIS	DG informato entro 1h. Contenimento urgente. Valuzione obbligo pre-notifica ACN. Coinvolgere DPO per dati pazienti.
P3	**MEDIO**	Degrado prestazioni sistemi clinici; anomalie accesso cartelle; blocco parziale prenotazioni	Phishing confermato senza laterale; vuln critica sfruttata su sistema non critico; account singolo compromesso	Notifica Direttore UOC Sistemi Informativi entro 2h. Analisi entro 4h. Remediation entro 24h. Monitorare evoluzione a P2/P1.
P4	BASSO	Nessun impatto diretto su servizi clinici	Phishing bloccato; alert SIEM non confermato; violazione policy minore; quasi-incidente	Gestione ordinaria ICT. Documentare nel Registro Incidenti. Monitorare. Nessuna escalation immediata. Segnalare al CISO in report mensile.

6.2 Matrice di correlazione IS – Priorità

La seguente matrice correla le tipologie ACN con le priorità operative interne, tenendo conto dell'entità dell'impatto:

Tipo ACN	Con impatto su servizi critici	Con impatto su servizi secondari	Senza impatto clinico immediato
IS-1 (Riservatezza)	P1/P2 + Notifica ACN + Notifica Garante	P2 + Notifica ACN + Notifica Garante	P3 + Notifica ACN + Valuta Garante
IS-2 (Integrità)	P1/P2 + Notifica ACN + Notifica al Garante	P2 + Notifica ACN + Notifica al Garante	P3 + Notifica ACN + Valutazione per eventuale notifica al Garante
IS-3 (Livelli di Servizio)	P1 + Notifica ACN obbligatoria + Notifica al Garante	P2 + Notifica ACN + Notifica al Garante	P3 + Valuta Notifica ACN + Valutazione per eventuale notifica al Garante
IS-4 (Accesso non autorizzato)	P1/P2 + Notifica ACN + + Notifica al Garante	P2/P3 + Notifica ACN + Notifica al Garante	P3/P4 + Valuta Notifica ACN + Valutazione per eventuale notifica al Garante

Dubbio sulla significatività — Principio di cautela

In caso di dubbio se un incidente sia da classificare come significativo (IS-1÷IS-4), l'ASL DEVE procedere con la pre-notifica entro 24h. Il CSIRT Italia non sanziona le notifiche cautelative inviate in buona fede. La mancata notifica di un incidente che si rivela successivamente significativo è invece sanzionata (Art. 36 D.Lgs. 138/2024: fino a 10.000.000 EUR o 2% fatturato globale per Soggetti Essenziali).

7. Obblighi di notifica

7.1 Notifica NIS2 all'ACN/CSIRT Italia (Art. 25 D.Lgs. 138/2024)

Per gli incidenti classificati come significativi (IS-1÷IS-4), l'ASL ha l'obbligo di notificare al CSIRT Italia secondo le seguenti fasi. I termini decorrono dal momento in cui l'ASL ha acquisito evidenza dell'incidente:

Fase	Termine	Canale e Responsabile	Contenuto minimo obbligatorio
PRE-NOTIFICA	**≤ 24 ORE**	Portale NIS: https://portale.acn.gov.it/ Responsabile: Referente CSIRT (o sostituto), Punto di contatto NIS2 (o sostituto)	Indicare: data/ora evidenza; tipo incidente (IS-1÷IS-4); sistemi/servizi ASL coinvolti; impatto stimato su erogazione servizi; se si ritiene possibile un atto illecito o malevolo; se potenziale impatto transfrontaliero; recapito Referente CSIRT ASL
NOTIFICA	**≤ 72 ORE**	Portale NIS: https://portale.acn.gov.it/ Responsabile: Referente CSIRT (o sostituto), Punto di contatto NIS2 (o sostituto)	Aggiornamento pre-notifica. Aggiungere: data/ora rilevamento; asset impattati; vettore d'attacco (se noto); misure di contenimento intraprese e pianificate; IoC disponibili (IP, hash, ransom note); evidenze rilevanti (sample malware); valutazione iniziale gravità e impatto
NOTIFICA INTERMEDIA	Su richiesta ACN	Portale NIS: https://portale.acn.gov.it/ Responsabile: Referente CSIRT (o sostituto), Punto di contatto NIS2 (o sostituto)	Aggiornamenti sullo stato di avanzamento della risposta, nuovi elementi identificati, cronoprogramma ripristino servizi clinici
RELAZIONE FINALE	**≤ 1 MESE dalla notifica**	Portale NIS: https://portale.acn.gov.it/ Responsabile: Referente CSIRT (o sostituto), Punto di contatto NIS2 (o sostituto)	Descrizione dettagliata dell'incidente; causa radice (root cause); tipo di minaccia; misure di attenuazione adottate e in corso; impatto transfrontaliero (se noto); lessons learned; misure preventive adottate per evitare recidive
RELAZIONE MENSILE (solo se incidente ancora in corso)	Mensile fino a chiusura	Portale NIS: https://portale.acn.gov.it/ Responsabile: Referente CSIRT (o sostituto), Punto di contatto NIS2 (o sostituto)	Aggiornamento mensile sui progressi, seguito da relazione finale entro 1 mese dalla conclusione della gestione

7.2 Notifica al Garante Privacy

In parallelo alla notifica NIS2, qualora l'incidente coinvolga dati personali di pazienti o altri interessati, l'ASL (quale Titolare del Trattamento) è soggetta all'obbligo di notifica al Garante Privacy ai sensi dell'Art. 33 GDPR. I due processi sono distinti e paralleli. La notifica viene gestita dall'Ufficio Privacy e Sicurezza delle Informazioni sotto coordinamento del DPO, secondo la procedura aziendale in vigore, reperibile al link: https://www.asl.pe.it/Sezione.jsp?idSezione=338#PROCEDURE.

7.3 Comunicazione ai destinatari dei servizi

Ai sensi dell'Art. 25, c.7, D.Lgs. 138/2024, sentito il CSIRT Italia, l'ASL comunica senza ingiustificato ritardo ai destinatari dei propri servizi (es. pazienti, medici di base, strutture convenzionate):

- Gli incidenti significativi che possono ripercuotersi negativamente sulla fornitura dei servizi sanitari;
- Le misure correttive o di mitigazione che i destinatari possono adottare in risposta a una minaccia informatica significativa;
- La natura della minaccia informatica significativa.

La comunicazione è gestita dall'Ufficio Relazioni con il Pubblico (URP) su impulso della Direzione Strategica.

Nel caso in cui gli incidenti comportino una violazione dei dati personali (Data Breach), l'Ufficio Privacy e Sicurezza delle Informazioni, con il supporto delle Strutture competenti e con il coordinamento del DPO Aziendale, predisporrà, senza ingiustificato ritardo, apposita comunicazione da rendere ai soggetti coinvolti come da procedura citata al punto 7.2.

8. Processo di gestione degli incidenti

Il processo di gestione degli incidenti si articola in 6 macro-fasi, descritte di seguito a livello di principio. I dettagli operativi, i flussi di lavoro (flowchart), le tabelle di attività con ID e responsabili, e i modelli documentali sono descritti nella Procedura Operativa correlata: PROC-INC-001 – Procedura di Gestione degli Incidenti di Sicurezza Informatica.

#	Fase	Obiettivo e output	Attori principali	Ref. FNCS
1	**Prevenzione e Misure Proattive**	Ridurre la probabilità e l'impatto degli incidenti attraverso monitoraggio continuo, patching, formazione, controlli di accesso. Output: piano di prevenzione aggiornato.	CISO, Direttore UOC Sistemi Informativi, tutto il personale	*GV.RM ID.RA PR.AT*
2	**Identificazione (Rilevazione e Segnalazione)**	Rilevare tempestivamente gli eventi di sicurezza tramite monitoraggio automatizzato (SIEM, XDR) e segnalazioni del	Tutto il personale, SOC, CSIRT Aziendale	*DE.AE DE.CM*

#	Fase	Obiettivo e output	Attori principali	Ref. FNCS
		personale. Aprire ticket ITSM. Output: segnalazione registrata.		
3	**Valutazione e Classificazione**	Determinare se l'evento è un incidente di sicurezza, classificarlo (IS-1÷IS-4 / P1÷P4), prioritizzarlo, valutare obbligo di notifica NIS2 e GDPR. Output: incidente classificato e prioritizzato.	Referente Cybersicurezza, Direttore UOC Sistemi Informativi, DPO	*DE.AE RS.AN*
4	**Notifica, Gestione e Risposta**	Contenimento (isolamento sistemi), analisi (root cause), raccolta evidenze forensi, eradicazione, notifica ACN/Garante, ripristino controllato. Output: incidente contenuto, notifiche inviate, sistemi ripristinati.	CSIRT Aziendale, Referente CSIRT, TGI, DS, DPO	*RS.MA RS.AN RS.CO RC.RP*
5	**Chiusura**	Formalizzare la chiusura, aggiornare il Registro Incidenti, trasmettere relazione finale al CSIRT Italia, comunicare la chiusura agli stakeholder interni. Output: incidente chiuso e documentato.	Referente Cybersicurezza, Referente CSIRT, DPO	*RS.IM RC.IM*
6	**Post-Incidente / Lessons Learned**	Analisi post-chiusura, Root Cause Analysis formale, aggiornamento Risk Register, POAM, procedure e politiche. Output: lessons learned documentate, misure preventive implementate.	CSIRT Aziendale, TGI	*GV.OC RS.IM*

Priorità alla continuità delle cure durante l'incidente

Per gli incidenti P1/P2 con impatto su sistemi critici, il Direttore Sanitario deve essere sempre coinvolto nella gestione dell'incidente, fin dal primo momento. Le procedure di fallback clinico (es. cartelle cliniche cartacee di emergenza, procedure manuali di laboratorio, deviazione ambulanze 118) devono essere attivate contestualmente alle azioni di contenimento ICT, non dopo.

9. Documentazione e conservazione

Ogni incidente deve essere documentato integralmente. La documentazione costituisce evidenza per eventuali audit istituzionali (ACN, Garante Privacy, autorità giudiziaria, forze dell'ordine), ispezioni, procedimenti legali e per il miglioramento continuo.

Documento	Contenuto	Conservazione minima	Classificazione
Registro degli Incidenti	Log di tutti gli incidenti (inclusi quasi-incidenti e P4) con ID univoco, date, classificazione, esito, azioni intraprese, responsabili	5 anni	**RISERVATO**
Report iniziale dell'incidente	Descrizione evento, sorgente, sistemi coinvolti, impatto stimato, prime evidenze, classificazione P/IS	5 anni	**RISERVATO**
Verbali TGI	Documentazione di ogni riunione del Team di Gestione Incidenti: decisioni prese, motivazioni, responsabili delle azioni	5 anni (esaminabili da ACN)	**RISERVATO**
Evidenze forensi	Log di sistema, memory dump, snapshot VM, network capture, sample malware, ransom note, hash SHA-256 delle copie forensi	12 mesi (storage isolato e immutabile)	**RISERVATO**
Copie notifiche ACN	Pre-notifica, notifica, relazioni intermedie e finale inviate al CSIRT Italia tramite portale ACN; ricevute di trasmissione	5 anni	**STRETTAMENTE RISERVATO**
Notifiche al Garante Privacy	Notifiche data breach inviate al Garante; comunicazioni agli interessati (se effettuate)	5 anni	**STRETTAMENTE RISERVATO**
Report finale / Lessons Learned	Root Cause Analysis, impatto definitivo, misure correttive, raccomandazioni, aggiornamenti a Risk Register e POAM	5 anni	**RISERVATO**

10. Sanzioni e non conformità

10.1 Sanzioni NIS2 (Art. 38 D.Lgs. 138/2024)

Per i Soggetti Essenziali della PA, le violazioni per la mancata osservanza degli obblighi imposti agli organi di amministrazione e direttivi e per l'inottemperanza delle disposizioni ACN sono punite con sanzioni pecuniarie da 25.000 a 125.000 euro.

È inoltre prevista la responsabilità dirigenziale, disciplinare e amministrativo-contabile del Direttore Generale e del personale con funzioni di rappresentanza, ai sensi dell'Art. 38, comma 7, D.Lgs. 138/2024, secondo le norme ordinarie sulla responsabilità dei dipendenti pubblici. Inoltre, è possibile l'erogazione di una sanzione accessoria di incapacità temporanea a svolgere funzioni dirigenziali (Art. 38, comma 6), applicabile in caso di mancato adempimento di una diffida dell'Autorità nazionale competente NIS ai sensi dell'art. 37, commi 6-7.

10.2 Sanzioni disciplinari interne

Il mancato rispetto della presente Politica da parte del personale ASL è soggetto a provvedimenti disciplinari in conformità al CCNL applicabile e al Regolamento Disciplinare aziendale.

In particolare possono essere passibili di provvedimento:

- La mancata segnalazione di un incidente rilevato;
- Lo spegnimento o la modifica intenzionale di sistemi compromessi, prima del nulla osta del CSIRT Aziendale, che porti alla distruzione di evidenze;
- La divulgazione non autorizzata di informazioni sull'incidente (potenziale responsabilità civile);

Per i fornitori, l'inadempienza agli obblighi contrattuali di notifica è causa di risoluzione contrattuale ex Art. 1456 c.c.

11. Revisione e aggiornamento

La presente Politica è soggetta a revisione con le seguenti modalità:

Trigger di revisione	Descrizione
Revisione periodica obbligatoria	Almeno ogni 12 mesi dalla data di emissione, indipendentemente dal verificarsi di eventi
Incidente significativo	Ogni incidente classificato IS-1÷IS-4 comporta una revisione della Politica entro 30 giorni dalla chiusura, per incorporare le lessons learned

Trigger di revisione	Descrizione
Variazioni normative	Es. alla presenza di nuove determinazioni ACN, di aggiornamenti D.Lgs. 138/2024, di nuovi provvedimenti Garante Privacy, o di nuove linee guida comunitarie
Cambiamenti organizzativi rilevanti	Alla nomina di nuove figure aziendali in materia di cybersicurezza o alla sostituzione delle figure NIS2 (Punto di Contatto, Referente CSIRT). All'avvenire di riorganizzazioni aziendali.
Cambiamenti tecnologici rilevanti	Introduzione di nuovi sistemi critici, migrazione cloud, nuovi contratti con fornitori di servizi critici.
Variazioni significative del profilo di rischio	Nuove minacce identificate nel threat landscape sanitario (es. nuovo vettore ransomware specifico per le Aziende Sanitarie, indicatori di compromissione segnalati da attori istituzionali)

Il processo di revisione si articola nelle fasi seguenti:

1. Redazione aggiornamento da parte del Referente per la Cybersicurezza;
2. Verifica da parte del Referente CSIRT e del DPO;
3. Approvazione da parte del Direttore Generale;
4. Distribuzione a tutto il personale e aggiornamento del Registro Documenti;
5. Formazione del personale sulle modifiche rilevanti.

Il Dirigente Amministrativo, con la presente sottoscrizione, attesta la regolarità tecnica e amministrativa nonché la legittimità del provvedimento

Il Dirigente Amministrativo
Marco De Benedictis
firmato digitalmente

Il Direttore dell'UOC Controllo di Gestione attesta che la spesa risulta corrispondente al bilancio di previsione dell'anno corrente.

Il Direttore

firmato digitalmente

Il Direttore dell'UOC Bilancio e Gestione Economica Finanziaria attesta che la spesa risulta imputata sulla voce di conto del Bilancio n.
Anno 2026

Il Direttore

firmato digitalmente

Ai sensi del D. Lgs. 502/92 e successive modificazioni ed integrazioni, i sottoscritti esprimono il seguente parere sul presente provvedimento:
Parere favorevole

IL DIRETTORE AMMINISTRATIVO
Dott. Francesca Rancitelli
firmato digitalmente

Parere favorevole

IL DIRETTORE SANITARIO
Dott. Rossano Di Luzio
firmato digitalmente

IL DIRETTORE GENERALE
Dott. Vero Michitelli
firmato digitalmente

Deliberazione n. 1374 **del** 24/08/2026 **ad oggetto:**

APPROVAZIONE DEI DOCUMENTI "REGOLAMENTO AZIENDALE IN MATERIA DI NOMINA E FUNZIONI DEGLI AMMINISTRATORI DI SISTEMA", "POLITICA AZIENDALE DI GESTIONE DEGLI INCIDENTI INFORMATICI" E "POLITICA AZIENDALE PER L'UTILIZZO DI DISPOSITIVI PERSONALI (BYOD)", NELL'AMBITO DEL SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI (SGSI) ADOTTATO DALLA ASL DI PESCARA CON DELIBERAZIONE N. 648 DEL 30/04/2026.

CERTIFICATO DI PUBBLICAZIONE

- Si attesta che il presente atto viene pubblicato, in forma integrale, all'ALBO ON LINE dell'ASL di Pescara (art. 32 L. 69/09 e s.m.i.), in data 24/8/2026 per un periodo non inferiore a 15 giorni consecutivi.

Atto soggetto al controllo della Regione (art. 4, co. 8 L. 412/91): NO

Il Funzionario Incaricato