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

DELIBERAZIONE DEL DIRETTORE GENERALE
AZIENDA SANITARIA LOCALE DI PESCARA

ANNO: 2026 N. 1764

Data 29/10/2026

OGGETTO: APPROVAZIONE DELLE POLITICHE DI SICUREZZA INFORMATICA DI AMBITO, DELLE RELATIVE PROCEDURE, DEL PIANO DI GESTIONE DEI RISCHI, DEL PIANO PROGRAMMATICO PER LA SICUREZZA INFORMATICA E DEL PIANO DI FORMAZIONE, IN ATTUAZIONE DELLA "POLITICA AZIENDALE PER LA SICUREZZA DEI SISTEMI, DEI DATI E DELLE INFORMAZIONI" E DEL D.LGS. 138/2024.

IL DIRETTORE GENERALE

OGGETTO: APPROVAZIONE DELLE POLITICHE DI SICUREZZA INFORMATICA DI AMBITO, DELLE RELATIVE PROCEDURE, DEL PIANO DI GESTIONE DEI RISCHI, DEL PIANO PROGRAMMATICO PER LA SICUREZZA INFORMATICA E DEL PIANO DI FORMAZIONE, IN ATTUAZIONE DELLA "POLITICA AZIENDALE PER LA SICUREZZA DEI SISTEMI, DEI DATI E DELLE INFORMAZIONI" E DEL D.LGS. 138/2024.

PREMESSO che:

- il decreto legislativo 4 settembre 2024, n. 138, di recepimento della direttiva (UE) 2022/2555 (c.d. NIS2), individua le aziende sanitarie quali soggetti essenziali e prevede, all'art. 24, l'adozione di misure tecniche, operative e organizzative adeguate e proporzionate per la gestione dei rischi per la sicurezza dei sistemi informativi e di rete e, all'art. 23, che gli organi di amministrazione e direttivi ne approvino le modalità di implementazione;
- la Determinazione del Direttore Generale dell'Agenzia per la cybersicurezza nazionale n. 379907/2025, applicabile dal 15 gennaio 2026, stabilisce all'Allegato 2 le misure di sicurezza di base per i soggetti essenziali e, in particolare, con la misura GV.PO-01, prevede l'adozione di politiche di sicurezza informatica per gli ambiti ivi indicati, approvate dagli organi di amministrazione e direttivi e rese note alle articolazioni competenti;
- la Legge 28 giugno 2024, n. 90, all'art. 8, comma 1, lettera a), attribuisce alla struttura per la cybersicurezza lo sviluppo delle politiche e delle procedure di sicurezza delle informazioni;
- la medesima Legge 90/2024, all'art. 8, comma 1, lettere b) e d), attribuisce alla struttura per la cybersicurezza, rispettivamente, la produzione e l'aggiornamento di un piano per la gestione del rischio informatico e di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture dell'amministrazione;
- l'art. 23, comma 2, del D.Lgs. 138/2024 prevede che gli organi di amministrazione e direttivi seguano una formazione in materia di sicurezza informatica e promuovano l'offerta periodica di una formazione coerente ai propri dipendenti;

RICHIAMATE:

- la Deliberazione n. 1802 del 04/12/2024, con la quale è stata individuata nella UOC Sistemi Informativi la struttura per la cybersicurezza ed è stato nominato il Referente per la cybersicurezza;
- la Deliberazione n. 791 del 17/06/2025, di nomina del sostituto del punto di contatto;
- la Determinazione dirigenziale della UOC Sistemi Informativi n. 4362 del 16/12/2025, di designazione del referente CSIRT e del relativo sostituto;
- la Deliberazione n. 648 del 30/04/2026, di approvazione della "Politica aziendale per la sicurezza dei sistemi, dei dati e delle informazioni", che prevede l'adozione di apposite politiche per i singoli ambiti della sicurezza informatica;

– la Deliberazione n. 1374 del 24/08/2026, di approvazione del "Regolamento aziendale in materia di nomina e funzioni degli Amministratori di Sistema" (SGI-ADS-REG-001), della "Politica aziendale di gestione degli incidenti informatici" (SGI-INC-POL-001) e della "Politica aziendale per l'utilizzo di dispositivi personali (BYOD)" (SGI-BYOD-POL-001);

CONSIDERATO che:

– la UOC Sistemi Informativi ha predisposto le politiche di ambito, le procedure e i piani elencati nell'Allegato A, che, unitamente ai documenti approvati con la Deliberazione n. 1374/2026, coprono tutti gli ambiti previsti dalla misura GV.PO-01 dell'Allegato 2 della Determinazione ACN n. 379907/2025;

– la Politica aziendale di gestione degli incidenti informatici (SGI-INC-POL-001), approvata con la Deliberazione n. 1374/2026, è stata riesaminata e aggiornata (revisione 1.2) al fine di assicurarne la coerenza con il quadro documentale del Sistema di Gestione della Sicurezza delle Informazioni, costituito dalla Politica aziendale approvata con Deliberazione n. 648/2026 e dalle politiche di ambito di cui all'Allegato A, nonché con la Determinazione ACN n. 379907/2025, che ha sostituito la Determinazione ACN n. 164179/2025 in essa richiamata;

– i documenti sono stati redatti secondo criteri di essenzialità e proporzionalità, in coerenza con la Politica aziendale approvata con Deliberazione n. 648/2026, e la corrispondenza con i requisiti ACN è documentata in un'apposita matrice di tracciabilità agli atti della UOC Sistemi Informativi;

– il Piano programmatico per la sicurezza informatica (SGI-CON-PIA-001) individua gli interventi necessari per il completamento dell'attuazione delle misure di sicurezza di base, compresi i documenti attuativi richiamati dalle politiche, ed è sottoposto all'approvazione della Direzione Generale ai sensi dell'art. 17 della Politica aziendale approvata con Deliberazione n. 648/2026 e della misura ID.IM-01;

– il Piano di gestione dei rischi per la sicurezza informatica (SGI-RIS-PIA-001) definisce la metodologia di identificazione, analisi, ponderazione e trattamento dei rischi, comprensiva dei criteri di propensione e tolleranza al rischio, ed è sottoposto all'approvazione della Direzione Generale ai sensi degli artt. 6 e 12 della Politica aziendale approvata con Deliberazione n. 648/2026, del paragrafo 5.2 della Politica SGI-RIS-POL-001 e della misura GV.RM-03;

– il Piano di formazione in materia di sicurezza informatica (SGI-RUM-PIA-001) definisce destinatari, contenuti, modalità di erogazione e di verifica della formazione, compresa quella degli organi di amministrazione e direttivi, ed è sottoposto all'approvazione della Direzione Generale ai sensi dell'art. 64 della medesima Politica aziendale e della misura PR.AT-01;

– i documenti di cui all'Allegato A aggiornano e integrano, per le parti relative alla sicurezza degli strumenti informatici, il Regolamento approvato con Deliberazione n. 23 del 12/01/2016;

RITENUTO pertanto di proporre l'approvazione dei documenti di cui all'Allegato A, che costituisce parte integrante del presente provvedimento;

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

D E L I B E R A

Per tutto quanto sopra indicato e che qui si intende integralmente richiamato

1) di **APPROVARE** le politiche di sicurezza informatica di ambito, le procedure e i piani elencati nell'Allegato A, che costituisce parte integrante e sostanziale del presente atto, dando atto che la revisione 1.2 della Politica SGI-INC-POL-001 sostituisce la versione approvata con la Deliberazione n. 1374/2026;

2) di **DELEGARE** al Referente per la cybersicurezza l'adozione e l'aggiornamento delle procedure, degli elenchi, dei registri e dei modelli attuativi delle politiche, nonché del programma attuativo annuale della formazione, da trasmettere alla Direzione Strategica, secondo quanto previsto dalla Politica SGI-CON-POL-001, e di DARE ATTO che gli ulteriori piani per i quali la normativa o la Politica aziendale approvata con Deliberazione n. 648/2026 richiedono l'approvazione degli organi di amministrazione e direttivi saranno sottoposti alla Direzione Generale;

3) di **DARE ATTO** che i documenti di cui al punto 1) aggiornano e integrano, per le parti relative alla sicurezza degli strumenti informatici, la Deliberazione n. 23/2016, che resta applicabile per le sole parti non incompatibili;

4) di **DARE MANDATO** alla UOC Sistemi Informativi di trasmettere i documenti alle articolazioni competenti e di darne comunicazione al personale;

5) di **TRASMETTERE** copia della presente deliberazione a: Direzione Strategica; Direttori di UOC e Responsabili di UOSD; UOC Sistemi Informativi; UOC Ingegneria Clinica; UOC Servizi Tecnici e Manutentivi; UOSD Progettazioni e Nuove Realizzazioni; Ufficio Privacy e Sicurezza delle Informazioni e Responsabile della protezione dei dati; UOC Acquisizione Beni e Servizi; UOC Dinamiche del Personale; UOS Formazione e Ricerca; UOS Risk Management; UOC Affari Generali e Legali;

6) di **DARE ATTO** che dal presente provvedimento non derivano oneri aggiuntivi a carico del bilancio aziendale;

7) di **DISPORRE** la pubblicazione del presente provvedimento nell'Albo Pretorio on-line aziendale e nella sezione Amministrazione Trasparente del sito istituzionale, ai sensi della normativa vigente.

ALLEGATO A – Documenti approvati

Codice	Titolo	Ambito GV.PO-01 / misura ACN
SGI-GOV-POL-001	Politica di governance: organizzazione, ruoli e responsabilità per la sicurezza informatica	b
SGI-RIS-POL-001	Politica per la gestione del rischio per la sicurezza informatica	a
SGI-CON-POL-001	Politica per la conformità e l'audit di sicurezza	d
SGI-AST-POL-001	Politica per la gestione degli asset	f

Codice	Titolo	Ambito GV.PO-01 / misura ACN
SGI-VUL-POL-001	Politica per la gestione delle vulnerabilità	g
SGI-BCM-POL-001	Politica per la continuità operativa, il ripristino in caso di disastro e la gestione delle crisi informatiche	h
SGI-INC-POL-002	Politica per il monitoraggio degli eventi di sicurezza	o
SGI-FOR-POL-001	Politica per la sicurezza della catena di approvvigionamento	e
SGI-RET-POL-001	Politica per la protezione delle reti e delle comunicazioni	n
SGI-APP-POL-001	Politica per la sicurezza delle applicazioni e dei sistemi	m
SGI-CFG-POL-001	Politica per la gestione delle configurazioni	m
SGI-IAM-POL-001	Politica per la gestione delle identità digitali, dell'autenticazione e del controllo accessi	i
SGI-DAT-POL-001	Politica per la sicurezza dei dati	l
SGI-RUM-POL-001	Politica per la sicurezza delle risorse umane e la formazione	c, k
SGI-FIS-POL-001	Politica per la sicurezza fisica e ambientale	j
SGI-INC-POL-001	Politica aziendale di gestione degli incidenti informatici (revisione 1.2)	p
SGI-IAM-PROC-001	Procedura di gestione del ciclo di vita delle utenze	i
SGI-RIS-PIA-001	Piano di gestione dei rischi per la sicurezza informatica (metodologia)	a – GV.RM-03
SGI-CON-PIA-001	Piano programmatico per la sicurezza informatica	d – ID.IM-01
SGI-RUM-PIA-001	Piano di formazione in materia di sicurezza informatica	k – PR.AT-01, PR.AT-02

8) di **DARE ATTO** che il presente provvedimento, ai sensi dell'art.6 del regolamento interno approvato con deliberazione 28/06/20212 n. 705, è immediatamente esecutivo;

9) di **DARE ATTO** che della L.R. n. 10/2022, decorsi i termini di pubblicazione di cui alla L. 69/2009, il presente provvedimento sarà soggetto a pubblicazione dei soli indici, quali data, oggetto e unità operativa proponente.

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 Trattamento Economico del Personale Dipendente e Convenzionato attesta che la spesa risulta imputata sulla voce di conto del Bilancio n. «vocediconto»
Anno

Il Direttore

firmato digitalmente

IL DIRETTORE GENERALE

Dott. Vero Michitelli

firmato digitalmente

Deliberazione n. 1764 **del** 29/10/2026 **ad oggetto:**

APPROVAZIONE DELLE POLITICHE DI SICUREZZA INFORMATICA DI AMBITO, DELLE RELATIVE PROCEDURE, DEL PIANO DI GESTIONE DEI RISCHI, DEL PIANO PROGRAMMATICO PER LA SICUREZZA INFORMATICA E DEL PIANO DI FORMAZIONE, IN ATTUAZIONE DELLA "POLITICA AZIENDALE PER LA SICUREZZA DEI SISTEMI, DEI DATI E DELLE INFORMAZIONI" E DEL D.LGS. 138/2024.

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 30/10/2026 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