

REGIONE DEL VENETO



ULSS7
PEDEMONTANA

Via dei Lotti, n. 40
36061 Bassano del Grappa (VI)
Codice fiscale e partita IVA 00913430245

N. 1589 DEL 13/10/2026

DELIBERAZIONE
del

DIRETTORE GENERALE

Nominato con D.P.G.R. n. 21 del 28/02/2026

Coadiuvato dai sigg.:

DIRETTORE AMMINISTRATIVO

dott.ssa LAURA ESPOSITO

DIRETTORE SANITARIO

dr. ANTONIO DI CAPRIO

DIRETTORE DEI SERVIZI SOCIO – SANITARI

dott.ssa PAOLA VESCOVI

OGGETTO: APPROVAZIONE DOCUMENTI CYBERSECURITY- D.LGS 138/24 (NIS2) E L. 90/24

IL DIRETTORE GENERALE
DELL'AZIENDA ULSS 7 PEDEMONTANA
dott. Giovanni Carretta

Documento informatico firmato digitalmente ai sensi del D. Lgs n. 82/2005, del T.U. n. 445/2000 e norme collegate, il quale sostituisce il documento cartaceo e la firma autografa; il documento informatico è conservato digitalmente negli archivi informatici dell'Azienda.

Proponente: UOC SISTEMI INFORMATIVI
Anno Proposta: 2026 Numero Proposta: 1667/26

Il Direttore dell'UOC Sistemi Informativi, nonché Responsabile del procedimento, attesta che la presente proposta di deliberazione è stata regolarmente istruita nel rispetto della vigente normativa nazionale, regionale e regolamentare: f.to. Alan Pettenà

Il Direttore dell'UOC Sistemi Informativi relaziona quanto segue:

Premesso che:

- con deliberazione del Direttore Generale n. 1387 del 24/08/2026 ad oggetto *"Definizione dei ruoli, responsabilità e poteri in materia di Cybersicurezza, ai sensi della Direttiva 'NIS2' e della Legge n. 90 del 28/06/2024"* si è provveduto a definire l'assetto di governance per la cybersicurezza, a nominare il Punto di Contatto NIS e il Referente per la Cybersicurezza, ed a costituire il "Comitato Esecutivo Cybersicurezza" assegnando al medesimo, tra l'altro, il compito di predisporre il documento organizzativo, le politiche e i piani di gestione del rischio entro la data del 14 ottobre 2026;
- con successiva deliberazione del Direttore Generale n. 1497 del 17/09/2026 ad oggetto *"Deliberazione n. 1387 del 24/08/2026 - Precisazioni sulla partecipazione del Responsabile della Protezione dei Dati (Data Protection Officer DPO) al Comitato Esecutivo Cybersicurezza e al Comitato di Gestione delle Crisi di Cybersicurezza ai sensi del Regolamento (UE) 2016/679 (GDPR)"* è stato precisato che la partecipazione del DPO avviene nell'ambito delle proprie competenze istituzionali di supervisione, consulenza e audit, con diritto di intervento e di proposta, ma senza diritto di voto deliberativo sulle decisioni gestionali dei Comitati.

Preso atto che:

- l'Azienda ULSS 7 Pedemontana è inserita nell'elenco dei soggetti NIS formalizzato con protocollo n. 0035109/25 del 14/04/2025, data dalla quale decorrono i 18 mesi per l'adeguamento normativo, ed è stata successivamente qualificata come Soggetto Essenziale (protocollo n. 0035322/26 del 14/04/2026), rendendo obbligatorio per l'Azienda il completamento dell'adozione e dell'attuazione delle politiche di gestione dei rischi e delle misure di sicurezza informatica, ai sensi del D.Lgs. 138/2024, entro e non oltre il 14 ottobre 2026;
- in data 15 settembre 2026, 2 ottobre 2026 e in data 9 ottobre 2026 si è regolarmente insediato e riunito il Comitato Esecutivo Cybersicurezza, sotto il coordinamento del Referente per la Cybersicurezza (Direttore UOC Sistemi Informativi), per esaminare e formulare la proposta dei documenti attuativi prescritti dalla normativa vigente e dalla citata deliberazione n. 1387/2026;
- nel corso delle sedute del 15/09/2026, del 02/10/2026 e del 09/10/2026 il Comitato Esecutivo Cybersicurezza ha formalmente approvato:
 1. il Regolamento del Comitato Esecutivo di Cybersicurezza;
 2. l'Elenco del Personale Membro del Comitato Cybersicurezza e del Modello Organizzativo Cybersicurezza;
 3. le Politiche di Sicurezza Informatica Aziendali, strutturate in conformità ai requisiti definiti dall'Allegato 2 della Determinazione ACN n. 379907/2025:
 - 00-AULSS7_Politica_di_sicurezza_informatica
 - 01-AULSS7_Politica_gestione_del_backup
 - 02-AULSS7_Politica_gestione_degli_asset
 - 03-AULSS7_Politica_gestione_della_crittografia
 - 04-AULSS7_Politica_Data_Governance
 - 05-AULSS7_Politica_gestione_delleidentità_e_degli_accessi_logici
 - 06-AULSS7_Politica_change_management
 - 07-AULSS7_Politica_vulnerability_management

- 08-AULSS7_Politica_sviluppo_sicuro
 - 09-AULSS7_Politica_log_management
 - 10-AULSS7_Politica_Threat_Intelligence
 - 11-AULSS7_Politica_di_valutazione_e_trattamento_del_rischio
 - 11_Allegato_A_Manuale_VERA
 - 12-AULSS7_Politica_Gestione_delle_terze_parti_ICT_IOMT_IOT
 - 12-AULSS7_Addendum_Requisiti_Cybersicurezza.
4. i Piani Aziendali, strutturati in conformità ai requisiti definiti dall'Allegato 2 della Determinazione ACN n. 379907/2025:
- 11-AULSS7_Piano_VR_TR_AR che comprende la valutazione del rischio, piano trattamento del rischio e il piano di adeguamento;
 - 07-AULSS7_Piano di gestione delle vulnerabilità;
 - AULSS7_Piano di continuità operativa;
 - AULSS7_Piano di ripristino in caso di disastro;
 - AULSS7_Piano di gestione delle crisi;
 - AULSS7_Piano per la gestione degli incidenti di sicurezza informatica.
- il Piano formazione è stato precedentemente deliberato con delibera n. 2376 del 24/12/2025 e contiene argomenti di cybersicurezza.

Considerato che:

- i documenti esaminati e proposti dal Comitato Esecutivo Cybersicurezza nelle sedute del 15/09/2026, del 02/10/2026 e del 09/10/2026 rispondono integralmente ai requisiti normativi di cui alla L. n. 90/2024, al D.Lgs. n. 138/2024 ed alle Determine ACN, garantendo il rispetto della scadenza fissata al 14 ottobre 2026 dalla deliberazione n. 1387/2026;
- l'approvazione formale di tali atti costituisce un passaggio indispensabile per assicurare la piena operatività della struttura di cybersicurezza aziendale, promuovere l'accountability ed innalzare il livello di resilienza delle infrastrutture digitali e sanitarie dell'Azienda;
- la partecipazione ed il contributo del DPO ai lavori ed alla stesura della documentazione si sono svolti in conformità alle funzioni di consulenza, vigilanza e audit previste dagli artt. 38 e 39 del GDPR e richiamate dalla deliberazione n. 1497/2026;

Visti:

- il D.Lgs. n. 82 del 07/03/2005 e s.m.i. "Codice dell'amministrazione digitale" (CAD), ed in particolare l'art. 51;
- la Direttiva (UE) 2022/2555 ("NIS2") ed il D.Lgs. n. 138 del 04/09/2024 di recepimento nazionale, con specifico riguardo agli artt. 7 e 40;
- la Legge n. 90 del 28/06/2024 recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici", ed in particolare l'art. 8;
- la Determinazione ACN n. 38565 del 26/11/2024;
- la Determinazione ACN n. 379907 del 18/12/2025 recante "Misure di sicurezza di base a carico degli organi di amministrazione e direttivi e in materia di misure di gestione dei rischi per la sicurezza informatica";
- la Determinazione ACN n. 379887 del 18/12/2025 relativa alle modalità di utilizzo della piattaforma digitale, designazione del Punto di Contatto NIS, del Referente CSIRT e sostituti;
- le DGR n. 1174 del 27/09/2022 e n. 1024 del 22/08/2023 relative all'approvazione ed esecuzione del progetto CERT Regionale;

- la deliberazione n. 1790 del 24/10/2023 dell'Azienda ULSS 7 Pedemontana avente ad oggetto "Progetto computer emergency response team (CERT) regionale. Adesione e approvazione schema di convenzione con Regione del Veneto".

Per quanto sopra esposto, il Direttore dell'UOC Sistemi Informativi propone di:

- approvare formalmente, recependo la proposta formulata dal Comitato Esecutivo Cybersicurezza nelle sedute del 15 settembre 2026, 2 ottobre 2026 e del 9 ottobre 2026, la seguente documentazione aziendale, conservata agli atti del presente provvedimento:
 1. il Regolamento del Comitato Esecutivo di Cybersicurezza;
 2. l'Elenco del Personale Membro del Comitato Cybersicurezza e del Modello Organizzativo Cybersicurezza;
 3. le Politiche di Sicurezza Informatica Aziendali, strutturate in conformità ai requisiti definiti dall'Allegato 2 della Determinazione ACN n. 379907/2025:
 - 00-AULSS7_Politica_di_sicurezza_informatica
 - 01-AULSS7_Politica_gestione_del_backup
 - 02-AULSS7_Politica_gestione_degli_asset
 - 03-AULSS7_Politica_gestione_della_crittografia
 - 04-AULSS7_Politica_Data_Governance
 - 05-AULSS7_Politica_gestione_delle_identità_e_degli_accessi_logici
 - 06-AULSS7_Politica_change_management
 - 07-AULSS7_Politica_vulnerability_management
 - 08-AULSS7_Politica_sviluppo_sicuro
 - 09-AULSS7_Politica_log_management
 - 10-AULSS7_Politica_Threat_Intelligence
 - 11-AULSS7_Politica_di_valutazione_e_trattamento_del_rischio
 - 11_Allegato_A_Manuale VERA
 - 12-AULSS7_Politica_Gestione_delle_terze_parti_ICT_IOMT_IOT
 - 12-AULSS7_Addendum_Requisiti_Cybersicurezza;
 4. i Piani Aziendali, strutturati in conformità ai requisiti definiti dall'Allegato 2 della Determinazione ACN n. 379907/2025:
 - 11-AULSS7_Piano_VR_TR_AR che comprende la valutazione del rischio, piano trattamento del rischio e il piano di adeguamento;
 - 07-AULSS7_Piano di gestione delle vulnerabilità;
 - AULSS7_Piano di continuità operativa;
 - AULSS7_Piano di ripristino in caso di disastro;
 - AULSS7_Piano di gestione delle crisi;
 - AULSS7_Piano per la gestione degli incidenti di sicurezza informatica;
- di stabilire che la documentazione di cui al punto precedente è classificata come confidenziale. Se ne autorizza la diffusione al personale dipendente, ai collaboratori e ai fornitori autorizzati, limitatamente alle sezioni di rispettiva competenza operativa e nel rispetto dei vincoli contrattuali di riservatezza. Resta fatto assoluto divieto di divulgazione o trasmissione a qualsiasi altro soggetto terzo non autorizzato, fatte salve le comunicazioni obbligatorie alle Autorità competenti.
- di dare mandato al Referente per la Cybersicurezza (Direttore UOC Sistemi Informativi) ed ai singoli componenti del Comitato Esecutivo Cybersicurezza di garantire l'attuazione ed il periodico aggiornamento dei piani, del regolamento e delle politiche approvate;

IL DIRETTORE GENERALE

Vista la relazione e la proposta del Responsabile del procedimento.

Dato atto che il Responsabile del servizio competente ha attestato l'avvenuta regolare istruttoria della pratica, in ordine alla compatibilità con la vigente legislazione statale, regionale e regolamentare.

Vista l'attestazione in merito all'assumibilità della spesa proposta, sottoscritta dal titolare del budget.

Acquisito il parere favorevole dei Direttori Amministrativo, Sanitario e dei Servizi Socio-Sanitari, per quanto di rispettiva competenza.

DELIBERA

1. di approvare formalmente, recependo la proposta formulata dal Comitato Esecutivo Cybersicurezza nelle sedute del 15 settembre 2026, 2 ottobre 2026 e del 9 ottobre 2026, la seguente documentazione aziendale, conservata agli atti del presente provvedimento.

- il Regolamento del Comitato Esecutivo di Cybersicurezza;
- l'Elenco del Personale Membro del Comitato Cybersicurezza e del Modello Organizzativo Cybersicurezza;
- le Politiche di Sicurezza Informatica Aziendali, strutturate in conformità ai requisiti definiti dall'Allegato 2 della Determinazione ACN n. 379907/2025:
 - 00-AULSS7_Politica_di_sicurezza_informatica
 - 01-AULSS7_Politica_gestione_del_backup
 - 02-AULSS7_Politica_gestione_degli_asset
 - 03-AULSS7_Politica_gestione_della_crittografia
 - 04-AULSS7_Politica_Data_Governance
 - 05-AULSS7_Politica_gestione_delleidentità_e_degli_accessi_logici
 - 06-AULSS7_Politica_change_management
 - 07-AULSS7_Politica_vulnerability_management
 - 08-AULSS7_Politica_sviluppo_sicuro
 - 09-AULSS7_Politica_log_management
 - 10-AULSS7_Politica_Threat_Intelligence
 - 11-AULSS7_Politica_di_valutazione_e_trattamento_del_rischio
 - 11_Allegato_A_Manuale_VERA
 - 12-AULSS7_Politica_Gestione_delle_terze_parti_ICT_IOMT_IOT
 - 12-AULSS7_Addendum_Requisiti_Cybersicurezza;
- i Piani Aziendali, strutturati in conformità ai requisiti definiti dall'Allegato 2 della Determinazione ACN n. 379907/2025:
 - 11-AULSS7_Piano_VR_TR_AR che comprende la valutazione del rischio, piano trattamento del rischio e il piano di adeguamento;
 - 07-AULSS7_Piano di gestione delle vulnerabilità;

- AULSS7_Piano di continuità operativa;
 - AULSS7_Piano di ripristino in caso di disastro;
 - AULSS7_Piano di gestione delle crisi;
 - AULSS7_Piano per la gestione degli incidenti di sicurezza informatica.
2. di stabilire che la documentazione di cui al punto precedente è classificata come confidenziale. Se ne autorizza la diffusione al personale dipendente, ai collaboratori e ai fornitori autorizzati, limitatamente alle sezioni di rispettiva competenza operativa e nel rispetto dei vincoli contrattuali di riservatezza. Resta fatto assoluto divieto di divulgazione o trasmissione a qualsiasi altro soggetto terzo non autorizzato, fatte salve le comunicazioni obbligatorie alle Autorità competenti;
 3. di dare mandato al Referente per la Cybersicurezza (Direttore UOC Sistemi Informativi) ed ai singoli componenti del Comitato Esecutivo Cybersicurezza di garantire l'attuazione ed il periodico aggiornamento dei piani, del regolamento e delle politiche approvate;
 4. di incaricare l'U.O.C. proponente di pubblicare la presente deliberazione sul sito aziendale nella sezione Amministrazione Trasparente tramite il link di collegamento con la BDNCP, ai sensi dell'art. 37 del D.Lgs. n. 33/2013 e s.m.i. e, ai sensi dell'art. 28 del D.Lgs. 36/2023;
 5. di dare atto che la presente deliberazione viene pubblicata all'albo del sito istituzionale dell'Azienda per 10 gg. continuativi, inviata contestualmente al Collegio Sindacale e diventa esecutiva il giorno stesso della sua pubblicazione, come da norma regolamentare approvata con deliberazione n. 1386 del 22.07.2022.