



SERVIZIO SANITARIO NAZIONALE REGIONE
PIEMONTE

Azienda Sanitaria ZERO

Costituita con D.P.G.R. 18/02/2022 n.9

Codice Fiscale / P.I. 12685160017

Sede legale: Edificio "Farfalla"

Piazza Piemonte 1 - 10127 Torino

Deliberazione del Direttore Generale

Proponente: S.C. Sistema Informativo

OGGETTO: Costituzione dell'Unità di Crisi aziendale per la gestione degli incidenti di sicurezza informatica e delle situazioni di crisi cyber in attuazione del decreto legislativo 4 settembre 2024, n. 138, di recepimento della Direttiva (UE) 2022/2555 (NIS2). Nessuna spesa.

IL DIRETTORE GENERALE

dott. Massimo D'ANGELO

nominato con D.G.R. n. 31-2373 del 16/03/2026

Visto il D.Lgs. n. 502 del 30.12.1992 e successive modificazioni ed integrazioni;

Visto l'art. 1 della legge regionale 26 ottobre 2021, n. 26 che ha previsto l'istituzione dell'Azienda Sanitaria Zero, di seguito denominata Azienda Zero, quale ente del Servizio Sanitario Regionale dotato di personalità giuridica pubblica e di autonomia amministrativa, patrimoniale, organizzativa, contabile, gestionale e tecnica;

Visto il D.P.G.R. n. 9 del 18/2/2022 con cui è stata costituita, ai sensi e per gli effetti della citata legge regionale 26 ottobre 2021, n. 26, l'Azienda Sanitaria Zero;

Vista la delibera 101/01.00 del 09/04/2024 Recepimento D.G.R. n. 21-8343 del 25/03/2024 "*Atti aziendali delle AA.SS.RR - Azienda Sanitaria Regionale Zero. Atto nr. 0000281/01.00/2023 del 27/12/2023 integrato con Atto nr. 31/01.00/2024 del 09.02.2024 "Atto Aziendale dell'Azienda Sanitaria Zero della Regione Piemonte di cui alla deliberazione nr. 2/01.00/2022 del 13/06/2022 come integrata con deliberazione nr. 281/01.00/2023 del 27/12/2023 – aggiornamento". Recepimento regionale con prescrizioni ai sensi della D.C.R. n.167-14087 del 3.04.2012, all. A, Par. 5.1"*;

Visto il vigente regolamento che disciplina le competenze per l'adozione degli atti amministrativi adottato con delibera n.414/01.00/2024 del 30 dicembre 2024;

Presa visione della proposta del direttore della S.C. Sistema Informativo, Ing. Simona Iaropoli che di seguito si riporta:

"Premesso che:

- la crescente dipendenza dei processi istituzionali, amministrativi e sanitari dai sistemi informativi e dalle infrastrutture digitali rende necessario assicurare un adeguato livello di resilienza rispetto ad eventi e incidenti di sicurezza informatica;
- gli incidenti di sicurezza informatica possono determinare impatti significativi sulla disponibilità, autenticità, integrità o riservatezza dei dati e dei sistemi informativi e di rete, nonché sulla continuità dei servizi erogati dall'Azienda;

- le specificità delle funzioni esercitate da Azienda Zero, con particolare riferimento alle attività e ai servizi a valenza regionale e ai sistemi connessi all'emergenza sanitaria, richiedono, in presenza di eventi cyber di particolare rilevanza, un modello organizzativo in grado di assicurare tempestività decisionale, coordinamento delle strutture aziendali coinvolte e raccordo con i soggetti istituzionali competenti;
- la gestione delle situazioni di crisi derivanti da incidenti di sicurezza informatica può richiedere il coinvolgimento coordinato di competenze direzionali, informatiche, sanitarie, amministrative, giuridiche, comunicative e in materia di protezione dei dati personali.
- la Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 (c.d. Direttiva NIS2) ha introdotto un quadro comune volto a garantire un livello elevato di cybersicurezza nell'Unione europea, rafforzando, tra l'altro, gli obblighi in materia di gestione dei rischi per la sicurezza informatica, gestione e notifica degli incidenti e responsabilità degli organi di amministrazione e direzione;
- il decreto legislativo n. 138/2024, recante "Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibernsicurezza nell'Unione", ha dato attuazione nell'ordinamento nazionale alla predetta Direttiva, individuando l'Agenzia per la Cybersicurezza Nazionale (ACN) quale Autorità nazionale competente NIS e disciplinando gli obblighi posti in capo ai soggetti rientranti nel relativo ambito di applicazione;
- il decreto legislativo n. 138/2024 individua il Ministero della Salute quale Autorità di settore NIS per il settore sanitario, chiamata a supportare l'Autorità nazionale competente NIS e a concorrere all'efficace e coerente attuazione della disciplina nel settore di competenza;
- la Legge 28 giugno 2024, n. 90, recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici", ha ulteriormente rafforzato il quadro nazionale in materia di cybersicurezza, introducendo specifiche disposizioni finalizzate ad accrescere le capacità di prevenzione, gestione e risposta agli incidenti informatici;
- l'Agenzia per la Cybersicurezza Nazionale, nell'esercizio delle funzioni attribuitele dal decreto legislativo n. 138/2024, ha adottato i provvedimenti attuativi volti a definire termini, modalità e adempimenti a carico dei soggetti NIS, nonché le misure di sicurezza e gli obblighi in materia di gestione e notifica degli incidenti cui gli stessi sono tenuti ad adeguarsi;

Considerato che:

- Azienda Sanitaria Zero rientra nel perimetro di applicazione della disciplina NIS2 ed è pertanto tenuta ad adottare un sistema strutturato di governo della sicurezza informatica, assicurando l'individuazione delle responsabilità, la valutazione e gestione dei rischi cyber, l'adozione delle misure di sicurezza applicabili, la gestione degli incidenti, la continuità operativa in caso di crisi;
- con Deliberazione n. 0000357/02.06/2025 del 12/09/2025 è stato nominato il Referente per la cybersicurezza ai sensi dell'art. 8 della legge n. 90/2024 e, successivamente, con deliberazione n. 0000009/02.06/2026 del 15/01/2026, è stato individuato il relativo sostituto;
- con Protocollo n. 2025/0024930 del 02/10/2025 sono stati individuati e formalizzati i ruoli di Punto di Contatto, Sostituto del Punto di Contatto e Segretario, nell'ambito degli adempimenti connessi all'attuazione della normativa in materia di cybersicurezza;
- con Deliberazione n. 0000009/02.06/2026 del 15/01/2026, Azienda Sanitaria Zero ha altresì individuato nella S.C. Sistema Informativo la struttura aziendale deputata allo svolgimento delle funzioni previste dall'art. 8, comma 1, della legge n. 90/2024;
- considerato che con protocollo n. 2026/0034444 del 09/10/2026 è stata conferita delega di Referente CSIRT di Azienda Zero, con attribuzione delle relative funzioni operative previste

dalla normativa in materia di cybersicurezza, allegata alla presente quale parte integrante (allegato 1);

- in attuazione delle disposizioni di cui al decreto legislativo 4 settembre 2024, n. 138, e dei relativi provvedimenti attuativi, Azienda Sanitaria Zero ha provveduto, mediante il Portale dei Servizi dell'Agenzia per la Cybersicurezza Nazionale (ACN), alla comunicazione e al successivo aggiornamento delle informazioni relative ai soggetti aziendali cui sono attribuiti ruoli e responsabilità in materia di cybersicurezza, nel rispetto delle modalità e delle tempistiche previste dalla normativa vigente;
- nell'ambito dell'assetto organizzativo aziendale definito per la gestione della sicurezza informatica, si rende necessario prevedere un organismo di coordinamento strategico e direzionale, denominato Unità di Crisi aziendale, da attivare in occasione di incidenti di sicurezza informatica o di eventi di natura cyber che, per gravità, estensione, complessità o potenziale impatto sull'organizzazione e sulla continuità dei servizi, richiedano una gestione coordinata a livello aziendale;
- l'Unità di Crisi aziendale opera in raccordo con le strutture e i soggetti competenti in materia di sicurezza informatica e gestione degli incidenti, senza sostituirsi alle rispettive funzioni tecniche e operative, assicurando il coordinamento delle decisioni e delle attività sotto il profilo strategico, organizzativo e direzionale;
- l'attivazione dell'Unità di Crisi è finalizzata, in particolare, ad assicurare il coordinamento delle attività necessarie alla gestione degli eventi, la salvaguardia della continuità operativa e dell'erogazione dei servizi aziendali, il raccordo tra le strutture coinvolte, nonché il presidio degli adempimenti di notifica e comunicazione previsti dalla normativa vigente e delle interlocuzioni con le Autorità e gli ulteriori soggetti istituzionali competenti, nel rispetto delle competenze attribuite ai soggetti aziendali responsabili;
- alla luce del quadro normativo e organizzativo sopra richiamato, si rende pertanto necessario, nell'ambito delle misure adottate da Azienda Sanitaria Zero per l'attuazione della disciplina di cui al decreto legislativo n. 138/2024 (NIS2) e per il rafforzamento del sistema aziendale di gestione della sicurezza informatica, procedere alla formale costituzione dell'Unità di Crisi aziendale per la gestione degli incidenti di sicurezza informatica e delle situazioni di crisi cyber, costituita dai seguenti componenti permanenti:
 - o Direttore Generale, con funzioni di Presidente dell'Unità di Crisi;
 - o Direttore Sanitario;
 - o Direttore Amministrativo;
 - o Direttore della S.C. Sistema Informativo;
 - o Punto di contatto NIS2 di Azienda Zero o, in caso di indisponibilità, il relativo sostituto;
 - o Referente CSIRT di Azienda Zero.
- in relazione alla natura, alle caratteristiche e agli impatti dell'evento, è prevista la possibilità per il Presidente dell'Unità di Crisi di disporre la convocazione di uno o più dei seguenti componenti a chiamata:
 - o Direttore del Dipartimento Strutturale Management e Gestione Reti Emergenza;
 - o Responsabile della S.S.S. Comunicazione interna ed esterna;
 - o Responsabile dell'Ufficio Legale e Contenzioso;
 - o Responsabile della S.S.S. Affari Generali e Legali;
 - o Direttore della S.C. Gestione Amministrativa Servizi Sanitari;
 - o Responsabile della Protezione dei Dati personali – DPO aziendale;

- Direttore o Responsabile della struttura o delle strutture aziendali interessate dall'evento.
- il Presidente può altresì disporre, in relazione alle specifiche esigenze connesse all'evento, la partecipazione alle riunioni dell'Unità di ulteriori professionalità interne o esterne all'Azienda, con funzioni di supporto tecnico-specialistico;
- i componenti dell'Unità di Crisi sono individuati ratione officii e l'eventuale cessazione o variazione del titolare dell'incarico non comporta la necessità di modificare il presente provvedimento, subentrando automaticamente nell'Unità il nuovo titolare della relativa funzione;
- l'Unità di Crisi è attivata dal Direttore Generale, in qualità di Presidente, anche su segnalazione del Direttore della S.C. Sistema Informativo, del Punto di contatto NIS2, del Referente CSIRT aziendale o di altra struttura che rilevi un evento potenzialmente critico;
- l'attivazione dell'Unità di Crisi avviene, in particolare, in presenza di incidenti di sicurezza informatica che possano determinare o abbiano determinato rilevanti conseguenze sulla continuità dei servizi aziendali, sui sistemi informativi e di rete, sui dati trattati, sui servizi sanitari o di emergenza-urgenza, ovvero che possano assumere rilevanza ai fini degli obblighi previsti dalla disciplina NIS;
- l'Unità di Crisi assicura, in caso di incidente o situazione di crisi cyber, il coordinamento strategico e decisionale delle strutture aziendali coinvolte, al fine di garantire la gestione dell'evento, la continuità dei servizi, il ripristino delle attività e l'assolvimento degli eventuali adempimenti e obblighi di comunicazione conseguenti;
- le modalità di attivazione e funzionamento dell'Unità di Crisi e le relative attività sono definite nella documentazione predisposta da Azienda Zero nell'ambito del percorso di adeguamento alla Direttiva NIS2 e alle misure adottate dall'Agenzia per la Cybersicurezza Nazionale, nel rispetto delle competenze attribuite alle singole strutture e funzioni aziendali;
- la costituzione e la partecipazione all'Unità di Crisi non comportano la corresponsione di compensi, indennità o emolumenti aggiuntivi e il presente provvedimento non comporta nuovi o maggiori oneri a carico del bilancio aziendale;"

Dato atto che il presente provvedimento non comporta, ex se, oneri di spesa diretti;

Considerato che la formulazione della proposta di un atto deliberativo impegna la responsabilità del soggetto proponente circa la regolarità amministrativa del contenuto della deliberazione nonché la legittimità della stessa;

Acquisiti i pareri favorevoli espressi dal Direttore Amministrativo, dott.ssa Antonella Bogliolo e dal Direttore Sanitario, dott. Arturo Pasqualucci, a norma dell'art. 3 del d.lgs. 30 dicembre 1992 n. 502

D E L I B E R A

per le motivazioni espresse in premessa che integralmente si richiamano

- 1) di costituire l'Unità di Crisi aziendale per la gestione degli incidenti di sicurezza informatica e delle situazioni di crisi cyber, quale organismo di coordinamento strategico e direzionale di Azienda Zero, da attivare in presenza di eventi che, per gravità, estensione, complessità o potenziale impatto, richiedano una gestione coordinata a livello aziendale.
- 2) di stabilire che l'Unità di Crisi sia costituita dai seguenti componenti permanenti:
 - Direttore Generale, con funzioni di Presidente dell'Unità di Crisi;
 - Direttore Sanitario;

- Direttore Amministrativo;
 - Direttore della S.C. Sistema Informativo;
 - Punto di contatto NIS2 di Azienda Zero o, in caso di indisponibilità, il relativo sostituto;
 - Referente CSIRT di Azienda Zero (con delega operativa allegata alla presente quale parte integrante Allegato 1).
- 3)** di stabilire che, in relazione alla natura, alle caratteristiche e agli impatti dell'evento, il Presidente dell'Unità di Crisi possa disporre la convocazione di uno o più dei seguenti componenti a chiamata:
- Direttore del Dipartimento Strutturale Management e Gestione Reti Emergenza;
 - Responsabile della S.S.S. Comunicazione interna ed esterna;
 - Responsabile dell'Ufficio Legale e Contenzioso;
 - Responsabile della S.S.S. Affari Generali e Legali;
 - Direttore della S.C. Gestione Amministrativa Servizi Sanitari;
 - Responsabile della Protezione dei Dati personali – DPO aziendale;
 - Direttore o Responsabile della struttura o delle strutture aziendali interessate dall'evento.
- Il Presidente può altresì disporre, in relazione alle specifiche esigenze connesse all'evento, la partecipazione alle riunioni dell'Unità di ulteriori professionalità interne o esterne all'Azienda, con funzioni di supporto tecnico-specialistico.
- 4)** di stabilire che i componenti dell'Unità di Crisi siano individuati *ratione officii* e che l'eventuale cessazione o variazione del titolare dell'incarico non comporti la necessità di modificare il presente provvedimento, subentrando automaticamente nell'Unità il nuovo titolare della relativa funzione;
- 5)** di stabilire che l'Unità di Crisi sia attivata dal Direttore Generale, in qualità di Presidente, anche su segnalazione del Direttore della S.C. Sistema Informativo, del Punto di contatto NIS2, del Referente CSIRT aziendale o di altra struttura che rilevi un evento potenzialmente critico.
- 6)** di stabilire che l'attivazione dell'Unità di Crisi avvenga, in particolare, in presenza di incidenti di sicurezza informatica che possano determinare o abbiano determinato rilevanti conseguenze sulla continuità dei servizi aziendali, sui sistemi informativi e di rete, sui dati trattati, sui servizi sanitari o di emergenza-urgenza, ovvero che possano assumere rilevanza ai fini degli obblighi previsti dalla disciplina NIS;
- 7)** di stabilire che l'Unità di Crisi assicuri, in caso di incidente o situazione di crisi cyber, il coordinamento strategico e decisionale delle strutture aziendali coinvolte, al fine di garantire la gestione dell'evento, la continuità dei servizi, il ripristino delle attività e l'assolvimento degli eventuali adempimenti e obblighi di comunicazione conseguenti;
- 8)** di stabilire che le modalità di attivazione e funzionamento dell'Unità di Crisi e le relative attività siano definite nella documentazione predisposta da Azienda Zero nell'ambito del percorso di adeguamento alla Direttiva NIS2 e alle misure adottate dall'Agenzia per la Cybersicurezza Nazionale, nel rispetto delle competenze attribuite alle singole strutture e funzioni aziendali.
- 9)** di dare atto che la costituzione e la partecipazione all'Unità di Crisi non comportano la corresponsione di compensi, indennità o emolumenti aggiuntivi e che il presente provvedimento non comporta nuovi o maggiori oneri a carico del bilancio aziendale.
- 10)** di disporre la trasmissione del presente provvedimento ai componenti dell'Unità di Crisi, alle strutture aziendali interessate e al Punto di contatto NIS2 per gli adempimenti di competenza.
- 11)** di dare atto che il presente provvedimento, *ex se*, non comporta oneri di spesa;

12) di dichiarare la presente deliberazione immediatamente eseguibile, ai sensi dell'art. 28 della legge regionale 24 gennaio 1995, n. 10, in considerazione della necessità di garantire il tempestivo adempimento degli obblighi previsti dal decreto legislativo 4 settembre 2024, n. 138.

Firmatari:

Responsabile del procedimento: Ing. Simona Iaropoli

Proponente: direttore S.C. Sistema Informativo

Direttore amministrativo: dott.ssa Antonella BOGLIOLO *

Direttore sanitario: dott. Arturo PASQUALUCCI *

Direttore generale: dott. Massimo D'ANGELO

Estensore dell'atto: Ing. Lorenzo Borda - Collaboratore tecnico S.C. Sistema Informativo

* I pareri favorevoli dei Direttori amministrativo e sanitario sono confermati con sottoscrizione del presente atto ed il rinvio automatico ai motivi della proposta. **I pareri sfavorevoli sono esplicitamente motivati ed indicati in allegato.**

La presente copia e' conforme all'originale depositato presso gli archivi dell'Azienda ASL Citta' di Torino

A9-7D-DA-CF-B3-60-7B-BB-C2-42-FA-0C-9B-01-8D-CF-BD-F8-9B-5A

CAdES 1 di 4 del 13/10/2026 10:08:29

Soggetto: Simona Iaropoli
S.N. Certificato: 1D0CFCE
Validità certificato dal 12/09/2024 11:55:11 al 12/09/2027 00:00:00
Rilasciato da InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT

CAdES 2 di 4 del 13/10/2026 10:20:04

Soggetto: Antonella Bogliolo
S.N. Certificato: 208E5EC
Validità certificato dal 23/03/2026 14:41:56 al 23/03/2029 00:00:00
Rilasciato da InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT

CAdES 3 di 4 del 13/10/2026 10:21:18

Soggetto: Arturo Pasqualucci
S.N. Certificato: 1FE179E
Validità certificato dal 04/11/2025 13:03:24 al 04/11/2028 00:00:00
Rilasciato da InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT

CAdES 4 di 4 del 13/10/2026 10:24:13

Soggetto: Massimo D'Angelo
S.N. Certificato: 2083FB1
Validità certificato dal 18/03/2026 09:36:54 al 18/03/2029 00:00:00
Rilasciato da InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT



SERVIZIO SANITARIO NAZIONALE REGIONE PIEMONTE

Azienda Sanitaria ZERO

Costituita con D.P.G.R. 18/02/2022 n.9

Codice Fiscale / P.I. 12685160017

Sede legale: Edificio "Farfalla"

Piazza Piemonte 1 - 10127 Torino

DIREZIONE GENERALE

e-mail: direzione.generale@aziendazero.piemonte.it

pec: protocollo@pec.aziendazero.piemonte.it

Alla cortese attenzione

Dott. Claudio Graffone

E p.c.

Al Direttore

S.C. Sistemi Informativi

Ing. Simona Iaropoli

ATTO DI DELEGA OPERATIVA E DESIGNAZIONE DEL REFERENTE CSIRT

L'anno duemilaventisei il giorno nove del mese di ottobre il sottoscritto Massimo D'Angelo, nella qualità di Direttore Generale dell'Azienda Sanitaria Zero, nominato con D.G.R. n. 31-2373 del 16/03/2026.

VISTA la direttiva (UE) 2022/2555 (NIS2) relativa a misure per un livello comune elevato di cibersicurezza nell'Unione;

VISTO il D.Lgs. 4 settembre 2024, n. 138, in particolare gli articoli 23, 24, 25 e 26, per quanto applicabili all'Azienda;

VISTA la disciplina attuativa dell'Agenzia per la Cybersicurezza Nazionale (ACN), e in particolare la determinazione ACN n. 127437 del 13 aprile 2026, art. 7, in tema di Referente CSIRT e relativi sostituti;

RICHIAMATO l'Atto aziendale vigente e la disciplina interna in materia di competenze, procedimenti amministrativi e sicurezza informatica;

VISTO che con Deliberazione n. 0000357/02.06/2025 del 12/09/2025 è stato nominato il Referente per la cibersicurezza ai sensi dell'art. 8 della Legge n. 90/2024;

VISTO che con nota Prot. n. 2025/0024930 del 02/10/2025 sono stati individuati e formalizzati i ruoli di Punto di Contatto NIS, Sostituto del Punto di Contatto e Segretario, nell'ambito degli adempimenti connessi all'attuazione della normativa in materia di cibersicurezza;

VISTO che con Deliberazione n. 0000009/02.06/2026 del 15/01/2026 è stato individuato il sostituto del Referente per la cibersicurezza;

VISTO che il Punto di Contatto NIS aziendale, Ing. Simona Iaropoli, ha provveduto alla designazione del Referente CSIRT sul Portale ACN, come risulta dalla ricevuta attestante l'avvenuta modifica, acquisita agli atti con Prot. n. 2026/0003430 del 04/02/2026;

CONSIDERATA l'esigenza di formalizzare le funzioni operative attribuite al Referente CSIRT e di assicurare un adeguato coordinamento con le strutture aziendali competenti, al fine di garantire il tempestivo assolvimento degli obblighi di notifica degli incidenti significativi, l'efficace gestione delle interlocuzioni con CSIRT Italia, nonché la continuità operativa e la tracciabilità degli adempimenti previsti dalla normativa vigente;

DATO ATTO che la designazione del Referente CSIRT sul Portale ACN compete al Punto di Contatto NIS e che la presente delega interna non sostituisce tale adempimento;



SERVIZIO SANITARIO NAZIONALE REGIONE PIEMONTE

Azienda Sanitaria ZERO

Costituita con D.P.G.R. 18/02/2022 n.9

Codice Fiscale / P.I. 12685160017

Sede legale: Edificio "Farfalla"

Piazza Piemonte 1 - 10127 Torino

FERME RESTANDO le competenze e le responsabilità degli organi di amministrazione e direzione previste dall'art. 23 del D.Lgs. n. 138/2024.

DISPONE

di conferire al Dott. Claudio Graffone, Collaboratore Professionale Informatico, in servizio presso la S.C. Sistemi Informativi, la delega operativa quale Referente CSIRT aziendale, subordinatamente alla designazione sulla piattaforma ACN da parte del Punto di Contatto NIS. Il presente atto non equivale, da solo, alla designazione telematica prevista dall'ACN.

Il delegato cura, per conto dell'Azienda e nell'ambito dei poteri assegnati:

- a) l'interlocuzione tecnico-operativa con CSIRT Italia;
- b) la predisposizione e trasmissione delle notifiche degli incidenti ai sensi degli artt. 25 e 26 del D.Lgs. 138/2024, nei casi e nei termini applicabili;
- c) l'acquisizione e la verifica delle informazioni necessarie con le strutture tecniche e organizzative coinvolte;
- d) la gestione dei riscontri, aggiornamenti e comunicazioni successive;
- e) la tracciabilità documentale delle comunicazioni e degli adempimenti effettuati.
- f) ogni altra attività e adempimento connesso o conseguente agli obblighi previsti dalla normativa vigente in materia.

Il delegato informa tempestivamente il Direttore Generale, il Punto di Contatto NIS, il responsabile della sicurezza informatica e le altre funzioni aziendali competenti degli incidenti significativi e delle notifiche effettuate, secondo le procedure aziendali. Il delegato segnala senza indugio eventuali impedimenti o criticità rilevanti.

La delega ha natura organizzativa e operativa. Non comporta trasferimento delle responsabilità spettanti agli organi di amministrazione e direzione, né attribuzione autonoma del potere di assumere impegni di spesa, rappresentare legalmente l'Azienda o adottare atti riservati ad altri organi o dirigenti.

La delega decorre dalla data indicata in epigrafe e resta efficace fino a revoca, sostituzione o modifica delle attribuzioni aziendali, ferma la necessità di aggiornare tempestivamente i dati comunicati ad ACN.

Le attività sono svolte nel rispetto della normativa sulla protezione dei dati personali, degli obblighi di riservatezza e delle misure aziendali di sicurezza, con utilizzo dei soli canali autorizzati.

Il presente atto è trasmesso al delegato e al Punto di Contatto NIS per la conservazione agli atti e i conseguenti adempimenti.

Torino, 9 ottobre 2026

Il **Direttore Generale**
Massimo D'Angelo
(firmato digitalmente)

Per presa visione e accettazione
Referente CSIRT Dott. Claudio Graffone
(firmato digitalmente)

CLAUDIO
GRAFFONE
17:01:58
GMT+02:00

La presente copia e' conforme all'originale depositato presso gli archivi dell'Azienda ASL Citta' di Torino

EA-CD-09-3C-CE-F7-23-B4-78-8A-0B-E2-D0-18-FE-9C-7E-DA-0A-15

PAdES 1 di 2 del 09/10/2026 17:01:58

Soggetto: CLAUDIO GRAFFONE

S.N. Certificato: A64F2E9B

Validità certificato dal 09/10/2026 08:00:01 al 09/10/2029 08:00:01

Rilasciato da ArubaPEC S.p.A.

PAdES 2 di 2 del 09/10/2026 17:13:41

Soggetto: Massimo D'Angelo

S.N. Certificato: 2083FB1

Validità certificato dal 18/03/2026 09:36:54 al 18/03/2029 00:00:00

Rilasciato da InfoCert S.p.A.

La presente copia e' conforme all'originale depositato presso gli archivi dell'Azienda ASL Citta' di Torino

85-5B-0E-9B-9E-B3-75-77-6B-F4-AA-D2-D4-66-86-BB-E7-15-5A-C0

CAdES 1 di 4 del 13/10/2026 10:01:58

Soggetto: Simona Iaropoli
S.N. Certificato: 1D0CFCE
Validità certificato dal 12/09/2024 11:55:11 al 12/09/2027 00:00:00
Rilasciato da InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT

CAdES 2 di 4 del 13/10/2026 10:20:06

Soggetto: Antonella Bogliolo
S.N. Certificato: 208E5EC
Validità certificato dal 23/03/2026 14:41:56 al 23/03/2029 00:00:00
Rilasciato da InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT

CAdES 3 di 4 del 13/10/2026 10:21:21

Soggetto: Arturo Pasqualucci
S.N. Certificato: 1FE179E
Validità certificato dal 04/11/2025 13:03:24 al 04/11/2028 00:00:00
Rilasciato da InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT

CAdES 4 di 4 del 13/10/2026 10:24:14

Soggetto: Massimo D'Angelo
S.N. Certificato: 2083FB1
Validità certificato dal 18/03/2026 09:36:54 al 18/03/2029 00:00:00
Rilasciato da InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT
