REGIONE CAMPANIA
AZIENDA OSPEDALIERA DI RILIEVO NAZIONALE E DI ALTA SPECIALIZZAZIONE
"SANT'ANNA E SAN SEBASTIANO"
CASERTA

Deliberazione del Direttore Generale N. 630 del 30/05/2025

Proponente: Il Direttore UOC SERVIZI INFORMATICI AZIENDALI

Oggetto: AZIENDA OSPEDALIERA "SANT'ANNA E SAN SEBASTIANO" DI CASERTA – RECEPIMENTO SCHEMA DI ACCORDO DI COOPERAZIONE PROGETTO "CSIRT-CAMPANIA"

PUBBLICAZIONE
In pubblicazione dal 30/05/2025 e per il periodo prescritto dalla vigente normativa in materia (art.8 D.Lgs 14/2013, n.33 e smi)

ESECUTIVITA'
Atto immediatamente esecutivo

TRASMISSIONE
La trasmissione di copia della presente Deliberazione è effettuata al Collegio Sindacale e ai destinatari indicati nell'atto nelle modalità previste dalla normativa vigente. L'inoltro alle UU. OO. aziendali avverrà in forma digitale ai sensi degli artt. 22 e 45 D.gs. n° 82/2005 e s.m.i. e secondo il regolamento aziendale in materia.

UOC AFFARI GENERALI
Direttore Eduardo Chianese

ELENCO FIRMATARI

Gaetano Gubitosa - DIREZIONE GENERALE
Giovanni Sferragatta - UOC SERVIZI INFORMATICI AZIENDALI
Angela Annecchiarico - DIREZIONE SANITARIA
Amalia Carrara - DIREZIONE AMMINISTRATIVA
Eduardo Chianese - UOC AFFARI GENERALI

Oggetto: AZIENDA OSPEDALIERA "SANT'ANNA E SAN SEBASTIANO" DI CASERTA – RECEPIMENTO SCHEMA DI ACCORDO DI COOPERAZIONE PROGETTO "CSIRT-CAMPANIA"

Direttore UOC SERVIZI INFORMATICI AZIENDALI

a conclusione di specifica istruttoria, descritta nella narrazione che segue ed i cui atti sono custoditi presso la struttura proponente, rappresenta che ricorrono le condizioni e i presupposti giuridico-amministrativi per l'adozione del presente provvedimento, ai sensi dell'art. 2 della Legge n. 241/1990 e s.m.i. e, in qualità di responsabile del procedimento, dichiara l'insussistenza del conflitto di interessi, ai sensi dell'art. 6 bis della legge 241/90 e s.m.i.

Premesso che

- l'Agenzia per la Cybersicurezza Nazionale, nell'ambito della quale è istituito il CSIRT Italia, ha adottato le "Linee Guida per la realizzazione di CSIRT", prot. n. 21392 del 07/08/2023, come aggiornate in data 24 luglio 2024, rivolte alle organizzazioni orientate ad istituire o potenziare un Cyber Security Incident Response Team, seguendo le migliori prassi e standard internazionali e definendo i requisiti di squadre di pronto intervento informatico dedicate al rilevamento, all'analisi e alla risposta degli incidenti di sicurezza informatica, nonché ad attività di prevenzione e mitigazione del rischio cyber;
- le recenti disposizioni europee, come la Direttiva NIS2 (link) e le normative italiane di riferimento, quali ad esempio L. 90/2024 (link), impongono obblighi precisi sulla sicurezza delle reti, dei sistemi informativi e sulla protezione dei dati, obbligando le amministrazioni a dotarsi di strumenti adeguati alla prevenzione, gestione e risposta agli incidenti informatici;
- in linea con la Strategia Nazionale di Cybersicurezza 2022-2026, il Piano Operativo per la Digitalizzazione della Regione Campania 2023-2025 ed il "Tech Strategy Regionale sulla Cybersecurity" sulla strategia tecnologica regionale relativa alla sicurezza informatica, approvato con Delibera regionale n. 551/2024 l'Amministrazione regionale ha l'intenzione di istituire CSIRT-Regionale Federato, che faciliti la cooperazione tra diverse regioni o enti locali, con il ruolo di coordinare, supportare e monitorare le attività di prevenzione, risposta e ripristino degli incidenti critici di tipo cyber nell'ambito del dominio costituito dal Fruitore;
- la Regione Campania, è inserita nel quadro delle azioni previste al precedente punto e, avendo ottenuto il medesimo finanziamento, nell'ambito delle attività di consolidamento della sicurezza informatica regionale, ha istituito il progetto Computer Security Incident Response Team, denominato con l'acronimo CISRT Campania, con l'obiettivo di istituire una struttura tecnica di prevenzione, gestione e risposta agli incidenti informatici su tutto il territorio regionale;

Considerato che

- l'Ufficio Speciale per la Crescita e la Transizione Digitale della Regione Campania, con nota prot. n. 14537 del 29/04/2025 ha trasmesso l'Accordo di Cooperazione Orizzontale e relativi allegati, nel quale vengono regolati i rapporti tra le parti, nonché ha fornito le istruzioni operative per l'avvio delle attività prodromiche alla collaborazione di cui trattasi;

- la formalizzazione dell'adesione avviene mediante recepimento dell'Accordo di Cooperazione Orizzontale ai sensi dell'art. 15 della Legge 7 agosto 1990, n. 241 e dell'art. 7, comma 4, del D. Lgs. 31 marzo 2023 n. 36, adottando, tra l'altro, il presente atto deliberativo;

Letti
Lo schema di Accordo di Cooperazione Orizzontale ed i relativi allegati A e B;

Ritenuto
pertanto, di recepire lo schema di Accordo di Cooperazione Orizzontale ed i relativi allegati A e B e procedere alla contestuale adozione del presente provvedimento;

Attestata
la legittimità della presente proposta di deliberazione, che è conforme alla vigente normativa in materia;

PROPONE

1) di prendere atto della nota dell'Ufficio Speciale per la Crescita e la Transizione Digitale della Regione Campania n. 14537 del 29/04/2025;
2) di aderire al Computer Security Incident Response Team (CSIRT) della Regione Campania per le attività demandate all'Ufficio Speciale per la crescita e la transizione digitale" (60.11.00), giusta Delibera di Giunta regionale n. 551/2024;
3) di prendere atto che l'adesione al CSIRT della Regione Campania rientra nel progetto finanziato a valere sul Piano Nazionale di Ripresa e Resilienza (PNRR) – Missione 1, Componente 1, Investimento 1.5 "Cybersecurity" – "Progetto CSIRT- Campania" – CUP: B27H23002720006;
4) di recepire lo schema di Accordo di Cooperazione Orizzontale ai sensi dell'art. 15 della Legge 7 agosto 1990, n. 241 e dell'art. 7, comma 4, del D. Lgs. 31 marzo 2023 n. 36, per la realizzazione del progetto Computer Security Incident Response Team della Regione Campania ed i relativi allegati A e B che, acclusi al presente provvedimento, ne costituiscono parte integrante e sostanziale;
5) di dare mandato al dott. Giovanni Sferragatta, Direttore U.O.C. Servizi Informatici Aziendali nonché Referente per la Cybersicurezza di questa A.O.R.N. per l'attuazione delle azioni previste dall'Accordo di Cooperazione Orizzontale inerente il progetto CSIRT-Campania;
6) di trasmettere il presente provvedimento al Collegio Sindacale, come per legge, alle UU.OO.CC. Gestione Economico – Finanziaria, Provveditorato ed Economato e Programmazione e Controllo di Gestione;
7) di rendere il presente provvedimento immediatamente eseguibile considerata l'importanza evinta dalla medesima disposizione regionale.

IL DIRETTORE U.O.C. S.I.A.
dott. Giovanni Sferragatta

IL DIRETTORE GENERALE
Dr. Gaetano Gubitosa
individuato con D.G.R.C. n. 465 del 27/07/2023
immesso nelle funzioni con D.P.G.R.C. n. 80 del 31/07/2023

Vista la proposta di deliberazione che precede, a firma del Direttore U.O.C. Servizi Informatici Aziendali Dott. Giovanni Sferragatta;

Acquisiti i pareri favorevoli del Direttore Sanitario e del Direttore Amministrativo in modalità telematica (art. 6, punto 1, lett. e) del regolamento aziendale e sotto riportati:

Il Direttore Sanitario	Dr.ssa Angela Annecchiarico	Favorevole
Il Direttore Amministrativo	Avv. Amalia Carrara	Favorevole

DELIBERA

per le causali in premessa, che qui si intendono integralmente richiamate e trascritte, di prendere atto della proposta di deliberazione che precede e, per l'effetto, di:

1) **PRENDERE ATTO** della nota dell'Ufficio Speciale per la Crescita e la Transizione Digitale della Regione Campania n. 14537 del 29/04/2025;
2) **ADERIRE** al Computer Security Incident Response Team (CSIRT) della Regione Campania per le attività demandate all'Ufficio Speciale per la crescita e la transizione digitale" (60.11.00), giusta Delibera di Giunta regionale n. 551/2024;
3) **PRENDERE ATTO** che l'adesione al CSIRT della Regione Campania rientra nel progetto finanziato a valere sul Piano Nazionale di Ripresa e Resilienza (PNRR) – Missione 1, Componente 1, Investimento 1.5 "Cybersecurity" – "Progetto CSIRT- Campania" – CUP: B27H23002720006;
4) **RECEPIRE** lo schema di Accordo di Cooperazione Orizzontale ai sensi dell'art. 15 della Legge 7 agosto 1990, n. 241 e dell'art. 7, comma 4, del D.Lgs. 31 marzo 2023 n. 36, per la realizzazione del progetto Computer Security Incident Response Team della Regione Campania ed i relativi allegati A e B che, acclusi al presente provvedimento, ne costituiscono parte integrante e sostanziale;
5) **DARE MANDATO** al dott. Giovanni Sferragatta, Direttore U.O.C. Servizi Informatici Aziendali nonché Referente per la Cybersicurezza di questa A.O.R.N. per l'attuazione delle azioni previste dall'Accordo di Cooperazione Orizzontale inerente il progetto CSIRT-Campania;
6) **TRASMETTERE** il presente provvedimento al Collegio Sindacale, come per legge, alle UU.OO.CC. Gestione Economico – Finanziaria, Provveditorato ed Economato e Programmazione e Controllo di Gestione;
7) **RENDERE** il presente provvedimento immediatamente eseguibile considerata l'importanza evinta dalla medesima disposizione regionale.

Il Direttore Generale
Gaetano Gubitosa

Loo

ACCORDO DI COOPERAZIONE ORIZZONTALE

AI SENSI DELL' ART. 15 DELLA LEGGE 7 AGOSTO 1990, N. 241 E DELL'ART. 7, COMMA 4, DEL D.LGS. 31 MARZO 2023 N. 36

TRA

REGIONE CAMPANIA – UFFICIO SPECIALE PER LA CRESCITA E LA TRANSIZIONE DIGITALE (C.F. 80011990639), con sede legale in Napoli, Via Don Bosco, n. 9/F, rappresentato dal Direttore Generale, Dott. Massimo Bisogno, in virtù del mandato conferito con la D.G.R. n. 143 del 31/03/2021 e n. 370 del 25/07/2024, domiciliato presso la sede, in ragione della carica ed agli effetti del presente atto,

(di seguito, anche «**U.S. 11**»)

E

NOME P.A.L.(C.F. ……) con sede legale in ……., rappresentata del Direttore Generale, Dott._____, domiciliato presso la sede, in ragione della carica ed agli effetti del presente accordo, di seguito anche Fruitore

(di seguito, anche «**P.A.L.**» o «**Fruitore**»)

(di seguito, congiuntamente, anche «**Parti**»)

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 e che abroga la direttiva 95/46/CE («**GDPR**»);

VISTO il Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea;

VISTO il Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il Regolamento (UE) n. 526/2013;

VISTA la Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del Regolamento (UE) n. 910/2014 e della Direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148;

VISTA la Legge 7 agosto 1990, n. 241, recante «*Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*» e, in particolare, l'articolo 15 che disciplina gli «*Accordi fra pubbliche amministrazioni*» e attribuisce alle Amministrazioni Pubbliche la facoltà di concludere tra loro accordi di collaborazione per lo svolgimento di attività di interesse comune;

RILEVATO in particolare che, ai sensi dell'articolo 15, comma 1, Legge 7 agosto 1990, n. 241, «*(…) le amministrazioni pubbliche possono sempre concludere tra loro accordi per disciplinare lo svolgimento in collaborazione di attività di interesse comune*»;

VISTO il Decreto Legislativo 30 giugno 2003, n. 196 e ss.mm. recante: «*Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al 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 e che abroga la Direttiva 95/46/CE*»;

VISTO il Decreto Legislativo 7 marzo 2005, n. 82 «*Codice dell'amministrazione digitale*»;

VISTO il decreto Legislativo 18 maggio 2018, n. 65, recante "*Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione*";

VISTO il 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*";

VISTO il decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, recante "*Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*" che ha istituito l'Agenzia per la Cybersicurezza Nazionale (di seguito "ACN" o "Agenzia") e in particolare gli artt. 5, comma 2 e 7, comma 3;

VISTO l'articolo 7, comma 1, lettere m) e n), del suddetto decreto-legge n. 82 del 2021, che ha attribuito all'Agenzia tutte le funzioni in materia di cybersicurezza già attribuite all'Agenzia per l'Italia digitale e i compiti di cui all'articolo 33-septies, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, nonché la responsabilità di sviluppare "*capacità nazionali di prevenzione, monitoraggio, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici […]"*;

VISTO l'articolo 7, comma 1, lettera t), del citato decreto-legge n. 82 del 2021, che individua l'Agenzia quale autorità che "*promuove, sostiene e coordina la partecipazione italiana a progetti e iniziative dell'Unione Europea e internazionali, anche mediante il coinvolgimento di soggetti pubblici e privati nazionali, nel campo della cybersicurezza nazionale e dei correlati servizi applicativi […]*";

VISTO il decreto del Presidente del Consiglio dei ministri 9 dicembre 2021, n. 223, recante "Regolamento di organizzazione e funzionamento dell'Agenzia per la Cybersicurezza Nazionale" e, in particolare, l'articolo 5;

VISTO il Piano Nazionale di Ripresa e Resilienza (PNRR) approvato con Decisione del Consiglio ECOFIN del 13 luglio 2021 e notificato all'Italia dal Segretariato generale del Consiglio con nota LT161/21 del 14 luglio 2021;

VISTO il decreto del Ministro dell'economia e delle finanze 6 agosto 2021, relativo all'assegnazione delle risorse in favore di ciascuna Amministrazione titolare degli interventi del PNRR e corrispondenti milestone e target, che individua la Presidenza del Consiglio dei ministri quale Amministrazione titolare della Missione 1, Componente 1, Investimento 1.5 recante "Cybersicurezza";

VISTA la Determina del 18 gennaio 2022, n. 306, dell'Agenzia per la Cybersicurezza Nazionale («**ACN**»), recante l'adozione del modello per la predisposizione dell'elenco e della classificazione di dati e di servizi;

VISTO il Decreto del Direttore generale dell'ACN dell'8 febbraio 2023, prot. n. 5489, recante: «*Differimento dei termini per l'adeguamento delle infrastrutture per la pubblica amministrazione*»;

VISTA la Circolare dell'Agenzia per l'Italia Digitale del 14 giugno 2019, n. 1, recante: «*Censimento del patrimonio ICT delle Pubbliche Amministrazioni e classificazione delle infrastrutture idonee all'uso da parte dei Poli Strategici Nazionali*»;

VISTO il Decreto Legislativo 31 marzo 2023 n. 36, recante «*Codice dei contratti pubblici*» e, in particolare, il comma 4 dell'articolo 7, rubricato « *Principio di auto-organizzazione amministrativa*», secondo cui: «*La cooperazione tra stazioni appaltanti o enti concedenti volta al perseguimento di obiettivi di interesse comune non rientra nell'ambito di applicazione del codice quando concorrono tutte le seguenti condizioni: a) interviene esclusivamente tra due o più stazioni appaltanti o enti concedenti, anche con competenze diverse; b) garantisce la effettiva partecipazione di tutte le parti allo svolgimento di compiti funzionali all'attività di interesse comune, in un'ottica esclusivamente collaborativa e senza alcun rapporto sinallagmatico tra prestazioni; c) determina una convergenza sinergica su attività di interesse comune, pur nella eventuale diversità del fine perseguito da ciascuna amministrazione, purché l'accordo non tenda a realizzare la missione istituzionale di una sola delle amministrazioni aderenti; d) le stazioni appaltanti o gli enti concedenti partecipanti svolgono sul mercato aperto meno del 20 per cento delle attività interessate dalla cooperazione*»;

VISTA La Legge del 28 giugno 2024, n. 90 recante “Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici” interviene su vari fronti, tra cui la prevenzione degli attacchi informatici e la protezione delle infrastrutture critiche nazionali, rendendo obbligatoria la creazione di struttura interna dedicata alla cybersicurezza nelle Pubbliche Amministrazioni, che assuma un ruolo centrale nella protezione e gestione delle infrastrutture IT, all’interno della quale opera il referente per la cybersicurezza, individuato in ragione di specifiche e comprovate professionalità e competenze in materia di cybersicurezza;

VISTO il Decreto legislativo 4 settembre 2024, n. 138, recepisce la Direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell’Unione (Direttiva NIS 2), stabilisce misure volte a garantire un livello elevato di sicurezza informatica in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell’Unione europea in modo da migliorare il funzionamento del mercato interno e rafforza l’obbligo di designare specifiche figure di responsabilità, tra cui il CISO (Chief Information Security Officer), che sarà incaricato della supervisione e implementazione delle misure di sicurezza e dei Team dedicati alla gestione degli incidenti di sicurezza con una capacità di risposta rapida in caso di attacchi cyber;

RICHIAMATA la Strategia Nazionale di Cybersicurezza 2022-2026 e il relativo Piano di Implementazione definiscono come pianificare, coordinare e attuare misure tese al potenziamento del livello di maturità delle capacità cyber della Pubblica Amministrazione, assicurando una trasformazione digitale sicura e resiliente. In particolare, la Misura #33 avente ad oggetto “Accrescere le capacità di risposta e ripristino a seguito di crisi cibernetiche implementando una rete di CERT settoriali integrata con il CSIRT Italia, nonché un piano nazionale di gestione crisi che definisca procedure, processi e strumenti da utilizzare in coordinamento con gli operatori pubblici e privati

VISTO il Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021, che istituisce il dispositivo per la ripresa e la resilienza con l’obiettivo specifico di fornire agli Stati membri il sostegno finanziario al fine di conseguire le tappe intermedie e gli obiettivi delle riforme e degli investimenti stabiliti nei loro Piani Nazionali di Ripresa e Resilienza («**PNRR**»);

VISTO il Decreto Legge 31 maggio 2021, n. 77, convertito con modificazioni dalla Legge 29 luglio 2021, n. 108, recante «*Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure*», con cui, per il PNRR, vengono definiti i ruoli ricoperti dalle diverse amministrazioni coinvolte, nonché le modalità di monitoraggio del Piano e del dialogo con le Autorità europee e nel quale si prevedono misure di semplificazione che incidono in alcuni dei settori oggetto del PNRR al fine di favorirne la completa realizzazione;

VISTO l’art. 9, comma 1, del Decreto Legge 31 maggio 2021, n. 77, secondo cui: «*Alla realizzazione operativa degli interventi previsti dal PNRR provvedono le Amministrazioni centrali, le Regioni, le Province autonome di Trento e di Bolzano e gli enti locali, sulla base delle specifiche competenze istituzionali, ovvero della diversa titolarità degli interventi definita nel PNRR, attraverso le proprie strutture, ovvero avvalendosi di soggetti attuatori esterni individuati nel PNRR, ovvero con le modalità previste dalla normativa nazionale ed europea vigente*»;

VISTO altresì, l’art. 10, commi 1 e 2, del Decreto Legge 31 maggio 2021, n. 77, secondo cui: «*Per sostenere la definizione e l'avvio delle procedure di affidamento ed accelerare l'attuazione degli investimenti pubblici, in particolare di quelli previsti dal PNRR e dai cicli di programmazione nazionale e dell’Unione europea 2014-2020 e 2021-2027, le amministrazioni interessate, mediante apposite convenzioni, possono avvalersi del supporto tecnico-operativo di società in house qualificate ai sensi dell'articolo 38 del decreto legislativo 18 aprile 2016, n. 50.64. 2. L'attività di supporto di cui al comma 1 copre anche le fasi di definizione, attuazione, monitoraggio e valutazione degli interventi e comprende azioni di rafforzamento della capacità amministrativa, anche attraverso la messa a disposizione di esperti particolarmente qualificati*»;

VISTA la Missione 1 «*Digitalizzazione, innovazione, competitività, cultura e turismo*» del richiamato PNRR che, nell'ambito della Componente 1 «*Digitalizzazione, innovazione e sicurezza della pubblica amministrazione*» prevede l'Investimento 1.5 «*Infrastrutture Digitali*» e l’Investimento 1.2 «*Abilitazione e facilitazione migrazione al cloud*»;

VISTO il Decreto del Ministero dell'Economia e delle Finanze 6 agosto 2021, recante «Assegnazione delle risorse finanziarie previste per l'attuazione degli interventi del Piano Nazionale di Ripresa e Resilienza (PNRR) e ripartizione di traguardi e obiettivi per scadenze semestrali di rendicontazione», che individua la Presidenza del Consiglio dei Ministri - Ministro per l'Innovazione Tecnologica e la Transizione Digitale quale Amministrazione titolare della Missione 1 Componente 1;

VISTO l'avviso pubblico del 11/08/2023 dell'Agenzia per la Cybersicurezza nazionale, in qualità di Soggetto attuatore, per la presentazione di proposte di interventi volti all'attivazione e al potenziamento di CSIRT Regionali, ossia di strutture di "Computer Security Incident Response Team" incardinati presso le Amministrazioni regionali, per il rafforzamento delle capacità di prevenzione, gestione e risposta degli incidenti informatici, nell'ambito della Missione 1 Componete 1 – Investimento 1.5 "Cybersecurity" – Codice d'investimento M1C1I1.5 del PNRR finalizzato a contribuire all'attuazione di investimenti finalizzati al rafforzamento delle capacità tecniche nazionali in materia di prevenzione e risoluzione di incidenti cyber, mediante l'attivazione di squadre di pronto intervento informatico deputate alla gestione degli incidenti e degli attacchi informatici sui propri sistemi informativi. L'avviso è destinato a finanziare, mediante procedura a sportello, per un valore complessivo di 28M€ secondo l'ordine cronologico di presentazione delle Istanze di partecipazione e fino alla concorrenza delle risorse disponibili – progettualità cd. a regia volte all'attivazione o al potenziamento di Computer Security Incident Response Team (CSIRT) da costituirsi o già costituiti presso le Regioni e le Province autonome, coerentemente con i requisiti minimi individuati dalle "Linee Guida per la realizzazione di uno CSIRT";

CONSIDERATO che la proposta progettuale "CSIRT Campania" della Regione Campania, rivolta anche agli Enti Sanitari per l'implementazione deI servizi pubblici di loro competenza, è risultata tra le proposte ammesse in graduatoria, di cui all'avviso pubblico del 11/08/2023, totalmente finanziabili per un importo complessivo pari ad € 1.499.904,60

VISTA la Determina dell'Agenzia Nazionale per la Cybersicurezza prot. n. 0030697.30-11 -2023 di ammissione a finanziamento del progetto presentato dalla Regione Campania per un importo complessivo pari ad € 1.499.904,60

RILEVATO che:

- l'Agenzia per la Cybersicurezza Nazionale, nell'ambito della quale è istituito il CSIRT Italia, ha adottato le "Linee Guida per la realizzazione di CSIRT", prot. n. 21392 del 07/08/2023, come aggiornate in data 24 luglio 2024, rivolte alle organizzazioni orientate ad istituire o potenziare un Cyber Security Incident Response Team, seguendo le migliori prassi e standard internazionali e definendo i requisiti di squadre di pronto intervento informatico dedicate al rilevamento, all'analisi e alla risposta degli incidenti di sicurezza informatica, nonché ad attività di prevenzione e mitigazione del rischio cyber.
- le recenti disposizioni europee, come la Direttiva NIS2 (link) e le normative italiane di riferimento, quali ad esempio L. 90/2024 (link), impongono obblighi precisi sulla sicurezza delle reti, dei sistemi informativi e sulla protezione dei dati, obbligando le amministrazioni a dotarsi di strumenti adeguati alla prevenzione, gestione e risposta agli incidenti informatici.
- in linea con la Strategia Nazionale di Cybersicurezza 2022-2026, il Piano Operativo per la Digitalizzazione della Regione Campania 2023-2025 ed il "Tech Strategy Regionale sulla Cybersecurity" sulla strategia tecnologica regionale relativa alla sicurezza informatica, approvato con Delibera regionale n. 551/2024 l'Amministrazione regionale ha l'intenzione di istituire CSIRT Regionale Federato, che faciliti la cooperazione tra diverse regioni o enti locali, con il ruolo di coordinare, supportare e monitorare le attività di prevenzione, risposta e ripristino degli incidenti critici di tipo cyber nell'ambito del dominio costituito dal Fruitore.

VISTO il Regolamento regionale del 27/05/2020, n. 7 «Modifiche al regolamento regionale 15 dicembre 2011, 12 (Ordinamento amministrativo della Giunta regionale della Campania), con il quale è stato istituito l'Ufficio Speciale per la crescita e la transizione digitale»;

VISTA la Delibera di Giunta Regionale n. 356 del 09/07/2020 con la quale è stato definito l'assetto organizzativo dell'Ufficio Speciale per la crescita e la transizione digitale" (60.11.00) con l'obiettivo di realizzare l'Agenda Digitale della Regione Campania, documento programmatico che traccia le strategie e le politiche in materia di *e-government* e di sviluppo digitale della Regione Campania;

VISTA la Delibera di Giunta Regionale n. 143 del 31/03/2021 con la quale è stato conferito l'incarico di responsabile dell'Ufficio Speciale per la Crescita e la Transizione digitale, codice 60.11.00, al dott. Massimo Bisogno.

CONSIDERATO che la Regione Campania ha realizzato un sistema di sicurezza informatica per proteggere i propri sistemi informativi e, contestualmente, ha anche incardinato nell'Ufficio Speciale per la crescita e la transizione al digitale il personale con specifiche competenze in materia di gestione digitale dei sistemi informativi, istituendo con D.D. n° 139 del 12/10/2022 il Security Operation Center (SOC), costituito da personale interno all'Ente con esperienza diretta nel campo di applicazione delle tecnologie informatiche per la sicurezza, che ha come obiettivo quello di innalzare il livello di resilienza cibernetica dei servizi critici erogati ai cittadini, con particolare attenzione ai settori dei trasporti e della sanità, attraverso la protezione degli asset, delle infrastrutture IT e dei sistemi posti alla base dell'erogazione di suddetti servizi da minacce di natura cyber;

VISTA la Delibera di Giunta Regionale n. 551 del 24 ottobre 2024, con la quale è stato stabilito di istituire il Computer Security Incident Response Team (CSIRT) della Regione Campania demandando all'Ufficio speciale per la crescita e la transizione digitale, anche in qualità di RTD dell'Ente, tutti gli adempimenti necessari per l'attivazione del CSIRT nonché, le modalità di integrazione per lo svolgimento delle funzioni regionali assegnate in qualità di Autorità di settore dalla disciplina NIS;

RILEVATO che con la Delibera di Giunta Regionale n. 551 del 24 ottobre 2024, è stato disposto:

a) 4. di istituire il Computer Security Incident Response Team (CSIRT) della Regione Campania demandando all'Ufficio speciale per la crescita e la transizione digitale, anche in qualità di RTD dell'Ente, tutti gli adempimenti necessari per l'attivazione del CSIRT nonché, le modalità di integrazione per lo svolgimento delle funzioni regionali assegnate in qualità di Autorità di settore dalla disciplina NIS;

b) 5. di stabilire che il CSIRT, in fase di avvio, svolga la propria attività con riferimento alle strutture della Regione Campania, con possibilità futura di integrare ed ampliare la realizzazione di un servizio a supporto del territorio nella prevenzione e risposta agli incidenti di sicurezza informatica, operando in un'ottica di filiera, con tutti gli Enti del territorio regionale;

c) 7. di demandare all'Ufficio speciale per la crescita e la transizione digitale l'individuazione della struttura di governo, le tecnologie, la precisazione dei servizi inclusi nella soluzione di CERT Regionale, dei ruoli e delle tempistiche di attuazione, la definizione della constituency, delle competenze e professionalità, delle responsabilità e modalità di funzionamento del modello organizzativo, dei processi di attivazione e coordinamento per la gestione di eventuali incidenti di sicurezza, delle regola e dei costi di gestione annuali, dei modelli di adesione e di partecipazione alla spesa;

VISTO il Decreto Dirigenziale n. 379 del 31.12.2024 che ha approvato i documenti di cui al punto successivo per garantire un efficace funzionamento del CSIRT regionale e gestione della sicurezza informatica a livello regionale - "PNRR - M1C1 - Investimento 1.5 "Cybersecurity" - Codice d'investimento M1C1I 1.5. Progetto "CSIRT - Campania" - CUP B27H23002720006

RILEVATO che il Decreto Dirigenziale n. 379 del 31.12.2024, al fine di garantire un funzionamento efficace ed efficiente dello CSIRT regionale, nonché conforme agli obiettivi di sicurezza informatica individuati dalla normativa comunitaria, nazionale e regionale, e assicurare che tutte le parti coinvolte abbiano una definizione chiara dei ruoli e delle responsabilità, facilitando la risposta alle minacce informatiche e migliorando la gestione degli incidenti attraverso una comunicazione e una governance ben strutturate, ha approvato i seguenti documenti che rappresentano i processi interni a Regione Campania e che potranno essere oggetto di futura evoluzione dei servizi erogati verso la Constituency:

a) CSIRT_MACON_ID_01 - Mandato del CSIRT e Constituency: il documento fornisce una chiara definizione delle funzioni e degli obiettivi del CSIRT, stabilendo le responsabilità e l'ambito di azione del team, nonché i soggetti e le organizzazioni che beneficeranno del servizio del CSIRT.

b) CSIRT_ORGAN_ID_01 - Modello Organizzativo del CSIRT: il documento definisce la struttura operativa del CSIRT, indicando come le risorse all'interno dell'organizzazione siano allocate in modo efficace per affrontare le minacce in tempo utile, attraverso la definizione di flussi di lavoro

chiari per la gestione degli incidenti, il monitoraggio delle minacce e il coordinamento con altre entità regionali o nazionali.

c) CSIRT_SERVI_ID_01 - Modello di Servizio del CSIRT: il documento descrive i servizi che il CSIRT offrirà alla Constituency, inclusi monitoraggio, rilevamento e risposta agli incidenti, bilanciando capacità, risorse e il tipo di supporto necessario alle strutture; CSIRT_AUDIT_PR_01 - Procedura di Gestione degli Audit Interni: il documento descrive la corretta implementazione delle procedure e delle politiche per garantire e valutare che il CSIRT stia operando in modo conforme agli standard di sicurezza e alle normative applicabili, consentendo di identificare e correggere tempestivamente eventuali inefficienze o problemi operativi.

d) CSIRT_COMUN_PR_01 - Procedura di Comunicazione interna ed esterna: il documento stabilisce le modalità di comunicazione del CSIRT con i suoi membri, le organizzazioni coinvolte, e il pubblico, per garantire che tutte le parti interessate siano informate tempestivamente sugli incidenti e le risposte, riducendo il rischio di disinformazione e per coordinare la risposta, mitigare i danni e proteggere la reputazione del CSIRT e della Regione.

DATO ATTO che le attività oggetto del presente accordo saranno svolte senza conseguimento di utili, né riconoscimento di alcuna remunerazione;

CONSIDERATO che il reciproco interesse delle Parti è finalizzato al perseguimento dei relativi obiettivi istituzionali, attraverso le necessarie forme di cooperazione, per la piena attuazione degli interventi alle stesse demandati dalla Delibera di Giunta Regionale n. 551 del 24 ottobre 2024, Computer Security Incident Response Team (CSIRT) della Regione Campania, con la pianificazione delle azioni, i tempi di esecuzione delle rispettive attività e l'impiego delle rispettive risorse, secondo le *milestone* e i *target* progettuali previsti e di ogni conseguente adempimento amministrativo;

RILEVATO che la predetta cooperazione è finalizzata all'esercizio coordinato delle funzioni istituzionali delle Parti, ai sensi dell'articolo 15, comma 1, della L. 241/1990 e garantisce l'effettiva partecipazione delle Parti allo svolgimento di compiti funzionali all'attività di interesse comune, in un'ottica esclusivamente collaborativa e senza alcun rapporto sinallagmatico tra prestazioni, ai sensi dell'art. 7, comma 4, lettera a), del D.Lgs. 36/2023;

RITENUTO di procedere alla stipula di un apposito accordo di cooperazione orizzontale, ai sensi degli articoli 15 della L. 241/1990 e 7, comma 4, del D.Lgs. 36/2023, approvato con Decreto Dirigenziale n. __ del ___;

Tutto ciò premesso, visto e considerato, le Parti, come sopra individuate, convengono e stipulano quanto segue

Articolo 1
(*Valore giuridico delle premesse e degli allegati*)

1. Le premesse e gli allegati, di seguito indicati, formano parte integrante e sostanziale del presente accordo di cooperazione orizzontale (di seguito, anche l'«**Accordo**»):

- Disciplinare Tecnico («**Allegato A**»);
- Nomina del responsabile del trattamento dei dati personali («**Allegato B**»).

2. Gli allegati di cui sopra vengono materialmente congiunti al presente Accordo.

Articolo 2
(*Definizioni*)

1. Ai fini dell'Accordo, si intende per:

a) «**ACN**»: l'Agenzia per la Cybersicurezza Nazionale, di cui al decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109;

b) «**Accordo**»: il presente atto, sottoscritto tra l'U.S. 11 e la P.A.L. ai sensi dell'art. 15 della L.

241/1990 e dell'art. 7, comma 4, del D.Lgs. 36/2023, finalizzato all'attivazione delle necessarie forme di cooperazione per la piena attuazione degli interventi di realizzazione del Computer Security Incident Response Team (CSIRT) della Regione Campania

c) «**CSIRT**»: Computer Security Incident Response Team con team organizzati di esperti di cybersicurezza il cui obiettivo principale è l'innalzamento del livello di cyber resilienza e la gestione degli incidenti informatici, per prevenire, mitigare e risolvere gli impatti;

d) «**Direttiva NIS2**»: Direttiva (UE) 2022/2555, recepita dal decreto legislativo del 4 settembre 2024, n. 138 (decreto NIS) e mira a stabilire una strategia comune di cybersecurity per tutti gli Stati membri, elevando i livelli di sicurezza dei servizi digitali su scala europea;

e) **«CSIRT Italia»**: organismo costituito presso l'Agenzia per la Cybersicurezza nazionale (ACN) i cui compiti sono definiti dal decreto Legislativo 18 maggio 2018, n. 65 e dal decreto del Presidente del Consiglio dei ministri 8 agosto 2019;

f) **«Fruitore**: Pubblica amministrazione Locale o Ente Sanitario Regionale, che fruisce dei servizi CSIRT

g) **«Linee guida CSIRT»:** documento approvato con Determina ACN prot. n. 21392 del 7 agosto 2023, che definisce il modello di riferimento per l'attivazione di un CSIRT e il potenziamento della maturità di quelli già in essere, mediante l'individuazione dei requisiti di dettaglio in termini di struttura organizzativa, competenze, strumenti e processi;

h) **AgID**»: l'Agenzia per l'Italia digitale, di cui all'articolo 19, del decreto-legge 22 giugno 2012, n. 83, convertito, con modificazioni, dalla legge 7 agosto 2012, n. 134;

i) «**Data center**»: Data center di Regione Campania denominato "Don Bosco", che rappresenta il nodo centrale dell'infrastruttura ICT regionale, responsabile dell'erogazione dei servizi offerti ai cittadini e alle imprese dalla PA, nonché del data center secondario di *disaster recovery*, sito in Fisciano (SA);

j) «**Disciplinare Tecnico**»: il documento che descrive e precisa le caratteristiche tecniche che i servizi oggetto del presente Accordo devono possedere e le ulteriori obbligazioni poste a carico delle Parti;

k) «**Interventi**»: l'insieme delle attività e dei servizi necessari all'attuazione del progetto CSIRT Campania;

l) **P.A.L.**: Pubblica Amministrazione locale: Agenzie e società in house della Regione Campania, delle Aziende Sanitarie Locali, delle Aziende Ospedaliere e degli IRCCS pubblici della Regione Campania;

m) «**PNRR**»: il Piano Nazionale di Ripresa e Resilienza, presentato alla Commissione in data 30 giugno 2021, valutato positivamente con Decisione del Consiglio ECOFIN del 13 luglio 2021 e notificato all'Italia dal Segretariato generale del Consiglio con nota LT161/21 del 14 luglio 2021;

n) «**Responsabili**»: i soggetti individuati dalle Parti, con compiti di supervisione ai fini dell'attuazione del presente Accordo;

Articolo 3
(*Finalità e ambito di applicazione*)

1. L'Accordo disciplina i rapporti tra le Parti e le reciproche obbligazioni finalizzate alla realizzazione delle attività demandate all'U.S. 11, giusto D.G.R. n. 551 del 24 ottobre 2024, Computer Security Incident Response Team (CSIRT) della Regione Campania. Le attività sono finalizzate a creare un contesto sistemico che favorisca lo sviluppo di iniziative sinergiche tra gli Enti operanti nel territorio regionale. Tali iniziative mirano a elevare i livelli di conoscenza, competenza e operatività in materia di sicurezza informatica. Inoltre, esse contribuiranno a potenziare le capacità di prevenzione e risposta a eventuali attacchi informatici, anche attraverso la creazione di una rete di presidio e mutuo soccorso territoriale, diffusa e operativa.

2. A seguito dell'adesione al CSIRT Regionale, gli Enti dovranno raggiungere i seguenti obiettivi: adozione dei requisiti di sicurezza AGID - requisiti minimi. Gli enti appartenenti al CSIRT dovranno soddisfare la lista di requisiti minimi come da linee guida AGID; adeguamento alla Direttiva NIS 2 (Direttiva UE 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 sulla sicurezza delle reti e delle informazioni) per gli enti operanti nei settori critici.
3. A tal fine, l'accreditamento degli Enti al CSIRT Regione Campania costituisce elemento strategico e condizione di sistema per il perseguimento degli obiettivi specifici del presente accordo, di seguito indicati:

a) analizzare la postura di sicurezza degli Enti e produrre un piano di potenziamento della cybersecurity;
b) fornire supporto nell'analisi dei dati relativi alle minacce informatiche emergenti e nella risoluzione degli incidenti di cyber security;
c) agevolare la diffusione di informazioni tempestive su nuovi scenari di rischio, attacchi in corso, trend di fenomeni cyber indirizzati a specifici settori e possibili impatti per il Fruitore e la loro utenza;
d) incentivare a livello locale l'applicazione dei processi di gestione della sicurezza, delle metodologie e delle metriche valutative per il governo della sicurezza cibernetica definite a livello nazionale;
e) facilitare le attività di prevenzione e monitoraggio sul territorio, agendo come unità capaci di esercitare un controllo più diretto a livello locale, mediante azioni di aggregazione dei servizi per il Fruitore;
f) collaborare e cooperare con le altre organizzazioni nazionali ed internazionali nel potenziamento e miglioramento della capacità difensiva del Fruitore in materia di cyber security;
g) accrescere le competenze specialistiche degli addetti alla sicurezza cibernetica e migliorare le attività di sensibilizzazione su questi temi;
h) aiutare il Fruitore a conformarsi alle normative vigenti in materia di sicurezza informatica, come la direttiva europea NIS e NIS2 e il decreto italiano sul perimetro di sicurezza nazionale cibernetica, che prevedono l'obbligo di notifica e di adozione di misure di sicurezza per gli operatori classificati come essenziali o importanti;

Sulla base delle risultanze dell'analisi sulla postura di sicurezza di cui al punto precedente, potranno essere definiti successivi obiettivi e specifiche iniziative ritenute significative e coerenti con le complessive finalità del presente accordo come indicate al primo capoverso del presente articolo.

4. Le Parti si impegnano a gestire in modo coordinato e sistemico la realizzazione delle iniziative, garantendo condizioni di efficacia ed efficienza. I servizi oggetto del presente Accordo concernono:
   - Assessment della postura di sicurezza propedeutico all'accreditamento
   - Portale WEB del CSIRT Regione Campania
   - Eventi di training e awareness
   - Report e alert di Cyber Threat Intelligence

Di seguito sono riportati gli ulteriori servizi offerti dal CSIRT di Regione Campania cui gli Enti avranno la possibilità di accedere a seguito della loro progressiva attivazione.

- Knowledge Transfer
- Gestione delle Vulnerabilità
- Situational Awareness
- Risposta agli Incidenti di Sicurezza
- Gestione degli Eventi e degli Incidenti di sicurezza informatica

I summenzionati servizi e le rispettive modalità di erogazione sono declinati all'Allegato A che costituisce parte integrante del presente accordo.

Articolo 4

(*Modalità operative*)

1. Il fruitore manifesta la propria volontà di adesione al presente accordo compilando e sottoscrivendo la "istanza di adesione" di cui all'all'Allegato A.
2. Con l'istanza di adesione il fruitore richiede, altresì, di essere accreditato al CSIRT Regione Campania, trasmettendo i recapiti del Referente per la sicurezza informatica dell'Ente.
3. L'U.S.11, valutata l'istanza, comunicherà al Fruitore le modalità per la sottoscrizione dell'accordo.
4. Le modalità operative ed i servizi erogati dal CSIRT, sono indicati nel capitolato Tecnico che costituisce parte integrante e sostanziale del presente accordo.

Articolo 5
(*Obblighi delle Parti*)

1. Le Parti si obbligano ad agire con correttezza e lealtà per realizzare lo scopo del contratto e ad evitare comportamenti che ostacolino o rendano più difficile l'adempimento per l'altra parte.
2. Con la sottoscrizione dell'Accordo, l'U.S. - Ufficio Speciale per la Crescita e la Transizione Digitale di Regione Campania, in quanto Ente responsabile del governo del CSIRT Regionale, garantisce l'acquisizione e il coordinamento dei servizi necessari all'operatività del CSIRT di Regione Campania, nonché l'erogazione dei servizi di prevenzione e protezione dagli attacchi informatici.
3. L'Ufficio Speciale per la Crescita e la Transizione Digitale di Regione Campania, sarà responsabile della gestione operativa del CSIRT, compresa la progettazione, la configurazione e la gestione dell'infrastruttura di sicurezza interna, il monitoraggio costante degli eventi di sicurezza, la segnalazione tempestiva di incidenti e l'assistenza nella gestione di eventuali minacce alla sicurezza informatica, oltre che lo svolgimento di attività specifiche volte ad innalzare il livello di protezione informatica. In particolare:
    - il supporto nella valutazione dello scenario cyber, per individuare strategie di protezione e servizi sempre in linea all'evoluzione tecnologica;
    - la valutazione della maturità del CSIRT sulla base di modelli di settore (es. framework SIM3) e la garanzia del rispetto del livello target definito da Regione Campania;
    - il supporto ai membri della Constituency del CSIRT nella prevenzione, risposta e gestione degli incidenti di sicurezza;
    - il mantenimento e aggiornamento delle tecnologie a supporto per erogazione servizi del CSIRT;
    - la formazione e l'aggiornamento continuo del personale (MEMBRI CONSTITUENCY) del CSIRT.
4. Con la sottoscrizione dell'Accordo, il Fruitore si obbliga a:
    a) nominare un referente per la sicurezza delle informazioni, il quale dovrà interfacciarsi con i referenti del CSIRT di Regione Campania;
    b) individuare personale dedicato alla gestione dei servizi di sicurezza forniti dal CSIRT Regionale;
    c) condividere esperienze e formulare proposte in una logica di scambio di esperienze, favorendo il percorso di graduale implementazione del CSIRT Regione Campania ed ogni iniziativa finalizzata alla realizzazione degli obiettivi di cui all'art.3;
    d) consentire al CSIRT Regione Campania eventuali approfondimenti in merito alle caratteristiche tecniche e funzionali dei sistemi utilizzati e rendere disponibili dati di monitoraggio per lo sviluppo di servizi o l'implementazione di policy;
    e) assumere tutti gli atti necessari, in base alla propria natura e alla propria organizzazione, a realizzare le finalità dell'accordo.
5. Fermi restando i reciproci obblighi a carico delle Parti e individuati nel presente paragrafo, resta inteso che l'U.S. 11, in ogni momento, potrà:

- modificare in qualsiasi momento, in ottemperanza alle nuove disposizioni di legge, le condizioni del servizio oggetto dell'Accordo.
-

Articolo 6
(*Corrispettivi dell'Accordo*)

1. Attesa la natura dell'Accordo, ciascuna Parte opera nell'ambito delle proprie competenze per la realizzazione delle finalità stabilite con il menzionato Accordo, destinando le occorrenti risorse umane e strumentali ritenute necessarie per la realizzazione delle azioni volte al raggiungimento delle comuni finalità.

2. I costi dei servizi sono sostenuti dalla Regione, il Fruitore non è soggetto a contributi economici di qualsivoglia natura.

3. Alla scadenza del presente Accordo, gli oneri economici connessi alla fruizione dei servizi saranno disciplinati mediante un nuovo accordo, contenente una dettagliata rappresentazione dei contributi dovuti e delle modalità di partecipazione da parte del Fruitore che vi aderirà. La determinazione dei contributi avverrà sulla base di parametri puntualmente indicati nell'accordo stesso, e i relativi importi saranno trasferiti all'U.S. 11 esclusivamente a titolo di rimborso delle spese e dei costi effettivamente sostenuti. Tali trasferimenti non avranno finalità di lucro, né costituiranno in alcun modo corrispettivo per prestazioni rese, in quanto l'Accordo è fondato su principi di cooperazione istituzionale e non configura un contratto a prestazioni corrispettive.

Articolo 7
(*Durata ed efficacia dell'Accordo*)

1. L'Accordo ha validità dalla sottoscrizione e fino alla data del 31/12/2026, salvo proroga espressamente prevista dalle parti con apposito atto decorrente dalla relativa sottoscrizione, fatto salvo l'esercizio del diritto di recesso ai sensi del successivo articolo 12, e impegna le Parti fino alla completa realizzazione degli Interventi.

Articolo 8
(*Riservatezza e Trattamento dei dati personali*)

1. Ai fini dell'esecuzione del presente Accordo, le Parti si obbligano a:

- osservare e rispettare le disposizioni del regolamento (UE) 2016/679 e dei corrispondenti e successivi provvedimenti regolamentari ed attuativi, ivi incluse tutte le successive modifiche e integrazioni;
- osservare e rispettare le disposizioni del D. Lgs. n. 196/2003, come modificato dal D. Lgs. n. 101/2018, ivi incluse tutte le successive modifiche e integrazioni;
- adottare tutte le misure di salvaguardia prescritte dalla normativa sopra citata;
- introdurre le ulteriori misure di salvaguardia disposte dal Garante per la protezione dei dati personali e dalle *best practices* internazionali e statali;
- rispettare nel tempo tutte le disposizioni emesse in tema di trattamento dei dati, anche laddove risultino maggiormente restrittive e vincolanti rispetto a quelle previste dalla normativa di riferimento vigente.

2. Con la sottoscrizione dell'Atto di nomina a responsabile del trattamento dei dati personali di cui all'«Allegato B» al presente Accordo, la Regione Campania, per il tramite dell'Ufficio Speciale per la crescita e la transizione digitale, in qualità di Titolare del trattamento dei dati personali, nomina XXX Il

Fruitore quale Responsabile del trattamento dei dati personali, ai sensi dell'articolo 28 del Regolamento (UE) 2016/679 sulla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati («**GDPR**»), per tutta la durata dell'Accordo. A tal fine, il Responsabile è autorizzato a trattare i dati personali necessari per l'esecuzione delle attività oggetto dell'Accordo e si impegna ad effettuare, per conto del Titolare, le sole operazioni di trattamento necessarie per fornire il servizio oggetto del presente Accordo, nei limiti delle finalità ivi specificate, nel rispetto del D. Lgs. n. 196/2003, del GDPR e delle istruzioni di seguito fornite.

3. Il Fruitore è consapevole che l'esecuzione dell'Accordo potrebbe comportare la conoscenza di dati e informazioni sensibili e/o riservate di titolarità della Regione, di soggetti terzi, pubblici o privati, nonché di persone fisiche e, pertanto, si impegna a:

- mantenere il massimo riserbo e segreto sul contenuto del presente Accordo, nonché sui dati e/o informazioni, ivi comprese quelle che transitano per le apparecchiature di elaborazione dei dati, di cui dovesse venire a conoscenza per effetto o semplicemente in occasione dell'esecuzioni del proprio incarico, ivi inclusi quelli di cui ai commi che precedono (a seguire le «**Informazioni Riservate**»);
- non divulgare le Informazioni Riservate in qualsiasi modo o forma;
- non farne oggetto di utilizzazione a qualsiasi titolo per scopi diversi da quelli strettamente necessari per l'esecuzione del presente Accordo.

4. Conseguentemente, il Fruitore si obbliga a mantenere riserbo assoluto in merito all'attività svolta, a tutelare adeguatamente le Informazioni Riservate, a non riprodurne copie né farne uso nel suo personale interesse o nell'interesse di terzi, e infine a non consentire che terzi ne facciano uso.

5. Gli obblighi sulle Informazioni Riservate di cui ai precedenti commi sussistono relativamente a tutto il materiale originario o predisposto in esecuzione del presente Accordo. Tale obbligo non sussiste tuttavia per i dati e le informazioni che:

- siano o divengano di pubblico dominio per fatti diversi dall'inadempimento della singola Parte ai propri obblighi di riservatezza e sempre che le Parti stesse abbiano dimostrato di aver posto in essere tempestivamente tutte le cautele necessarie a garantire la riservatezza delle Informazioni Riservate;
- siano divulgati a specifici soggetti sulla base di specifiche autorizzazioni;
- siano conosciuti dalla Parte ricevente, al di fuori di un obbligo di segretezza, prima della data di ricevimento o acquisizione;
- siano ricevuti o altrimenti conosciuti da una delle Parti, in modo lecito per fatto di terzi;
- siano informazioni richieste per legge o la cui rivelazione sia stata ordinata da un organo arbitrale o giudiziario, ovvero da autorità amministrative o governative e, in tal caso, solo dopo che la Parte richiesta abbia provveduto a darne sollecita informazione scritta all'altra Parte, così da permettere un'eventuale opposizione alla comunicazione ordinata e/o di assicurare un'adeguata protezione per la comunicazione richiesta.

6. Il fruitore relativamente alle Informazioni Riservate:

- si impegna ad adottare tutte le misure necessarie a trattare le predette Informazioni con la massima riservatezza, evitando ogni utilizzo di esse per scopi diversi, estranei o contrari a quelli strettamente necessari per l'esecuzione del presente Accordo;
- dovrà imporre l'obbligo di riservatezza a tutte le persone che, per ragioni del loro rapporto, vengano a conoscenza delle Informazioni Riservate;
- sarà responsabile per l'esatta osservanza di tali obblighi di riservatezza e segreto da parte dei propri dipendenti, consulenti e collaboratori e di ogni altra persona che per ragioni del proprio ufficio venga a conoscenza delle Informazioni Riservate in questione;
- comunicherà immediatamente per iscritto il fatto che qualsiasi Informazioni Riservata sia stata, o ragionevolmente si ritenga possa essere stata, o sia ragionevolmente probabile che possa essere

oggetto, di accesso o altro tipo di acquisizione da parte di soggetti diversi dalle persone autorizzate.

7. Le Parti dichiarano e garantiscono che tratteranno l'Accordo e il suo contenuto, nonché tutti gli altri atti, fatti e documenti connessi allo stesso o da questo direttamente o indirettamente derivanti, in maniera strettamente confidenziale, astenendosi, di conseguenza, fatto salvo quanto diversamente previsto nel presente articolo, dal fornire a chiunque qualunque notizia, informazione o dato senza il consenso dell'altra Parte, ad eccezione di quelli che fossero tenuti a fornire ad Autorità, Organi giudiziari e di controllo o ad altri in forza di disposizioni di legge, di regolamento, di ordine dell'Autorità Giudiziaria ovvero per l'esecuzione dell'Accordo.

Articolo 9
(*Comunicazioni e Responsabili dell'Accordo*)

1. Ai fini della corretta applicazione di quanto previsto nell'Accordo, le Parti nominano un proprio responsabile, qui di seguito indicato, giuridicamente preposto alla gestione dei rapporti e delle comunicazioni tra le stesse:

- per l'U.S. 11: Dott. Massimo Bisogno – massimo.bisogno@regione.campania.it;
- per il Fruitore: _____

1. Tutte le comunicazioni fra le Parti devono essere inviate ai rispettivi indirizzi di posta elettronica, qui di seguito precisati:

- per l'U.S. 11: us11@pec.regione.campania.it;
- per il Fruitore: _____

2. Le Parti si riservano di modificare, sempre previa comunicazione via PEC, gli indirizzi e i Responsabili sopra indicati.

Articolo 10
(*Variazioni dell'Accordo*)

1. Eventuali modifiche o integrazioni al presente Accordo potranno essere apportate esclusivamente per iscritto, mediante atto formalmente approvato e sottoscritto digitalmente da tutte le Parti.

2. Le Parti si impegnano a definire congiuntamente, ove necessario e con carattere provvisorio, modalità attuative parziali dell'Accordo che risultino, di volta in volta, più idonee a garantire il pubblico interesse e il buon andamento dell'azione amministrativa, anche attraverso la sottoscrizione di specifici addendum.

Articolo 11
(*Responsabilità e risoluzione dell'Accordo*)

1. Ciascuna delle Parti è responsabile del corretto e puntuale adempimento degli obblighi rispettivamente previsti dal precedente art. 4, nonché dal Disciplinare Tecnico, Allegato A al presente Accordo.

2. In caso di inadempimento di una delle obbligazioni previste nell'Accordo, per cause imputabili alla Parte inadempiente e tali da pregiudicare la realizzazione degli interventi di cui al presente accordo, la Parte non inadempiente invia formale sollecito ad adempiere all'altra Parte, a mezzo posta elettronica certificata, concedendo un termine congruo compatibile con le circostanze e le caratteristiche dell'obbligazione inadempiuta e, comunque, non superiore a 30 (trenta) giorni. Decorso inutilmente detto termine l'Accordo si intende risolto di diritto.

Articolo 12
(*Recesso*)

1. Le Parti hanno diritto di recedere dall'Accordo per gravi e giustificati motivi, previo preavviso scritto di almeno 30 (trenta) giorni.

2. Le Parti potranno altresì recedere dall'Accordo, in qualunque momento, qualora nel corso di svolgimento delle attività intervengano fatti o provvedimenti che modifichino la situazione esistente all'atto della stipula del predetto Accordo, o ne rendano impossibile o inopportuna la conduzione a termine.

Articolo 13
(*Controversie*)

1. Le controversie di qualsiasi natura che dovessero insorgere tra le Parti, in ordine all'interpretazione o all'esecuzione dell'Accordo o, comunque, direttamente o indirettamente connesse all'Accordo medesimo, sono devolute al foro di Napoli.

2. Resta inteso tra le Parti che l'insorgenza di eventuali controversie non pregiudicherà la regolare esecuzione delle attività regolate dall'Accordo, né consentirà alcuna sospensione delle stesse.

Articolo 14
(*Firma e registrazione*)

1. L'Accordo viene firmato digitalmente, ai sensi del D.P.R. 28 dicembre 2000, n. 445, del D.lgs. 7 marzo 2005, n. 82 e norme collegate, con sostituzione del testo cartaceo e della firma autografa ed è soggetto a registrazione in caso d'uso.

2. Le spese di registro e le altre eventuali inerenti soprattasse, sanzioni comunque relative all'Accordo, saranno interamente a carico della Parte che, non conformandosi a quanto in essa contenuto e previsto, darà causa al suo utilizzo ed alla sua eventuale produzione in giudizio.

Articolo 15
(*Norma di chiusura*)

1. Per quanto non espressamente previsto nei precedenti articoli, si rinvia alle norme euro-unitarie e nazionali di riferimento e, in particolare, agli articoli 15 della L. 241/1990 e 7, comma 4, del D.Lgs. 36/2023, oltre che alle norme del Codice civile, in quanto compatibili.

Articolo 16
(*Disposizioni finali*)

1. Le Parti convengono che l'Accordo è il risultato di un confronto volto al perseguimento di un interesse comune e di una specifica condivisione tra le stesse con riferimento ad ogni singola clausola.

2. L'Accordo si compone di 16 (sedici) articoli e 2 (due) allegati ed è sottoscritto digitalmente.

Letto, confermato e sottoscritto con firme digitali.

Napoli, […] 2025

REGIONE CAMPANIA – UFFICIO SPECIALE PER LA CRESCITA E LA TRANSIZIONE DIGITALE
Il Direttore Generale
Dott. MASSIMO BISOGNO

REGIONE CAMPANIA

CSIRT Regione Campania
Disciplinare Tecnico

Finanziato dall'Unione europea
NextGenerationEU

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

SOMMARIO

1. INTRODUZIONE 3
2. SERVIZI DEL CSIRT 4
2.1. Servizi a disposizione di tutti gli Enti del territorio 4
2.2. VALUTAZIONE MATURITÀ DEGLI ENTI CHE ADERISCONO ALL'INIZIATIVA 4
2.3. SERVIZI AD ATTIVAZIONE PROGRESSIVA 5
2.3.1. Modello di Delivery 6
2.3.2. Requisiti di Attivazione del Servizio 8
2.4. ALLEGATI 11
2.4.1. Istanza di adesione al CSIRT di Regione Campania 11
2.4.2. Selezione Servizi 12

1.INTRODUZIONE

L'obiettivo del Modulo Adesione Servizi è di fornire una panoramica chiara e dettagliata dei servizi disponibili offerti dal **CSIRT di Regione Campania**.

I servizi erogati dal **CSIRT di Regione Campania** identificano le specifiche operative offerte che compongono il **Modello di Servizio** (cfr. CSIRT_SERVI_ID_01 - Modello di Servizio del CSIRT).

Di seguito vengono riportati i **Servizi** del **CSIRT di Regione Campania offerti ai Membri della sua Constituency**:

2. SERVIZI DEL CSIRT

Il **CSIRT di Regione Campania** mette a disposizione dei membri della Constituency servizi e strumenti efficaci per un approccio integrato e focalizzato alla gestione delle minacce alla sicurezza informatica.

Sono state definite cinque aree di servizio, le quali delineano i settori operativi del **CSIRT di Regione Campania**, che saranno progressivamente attivate e messe a disposizione degli Enti della Constituency.

2.1. Servizi a disposizione di tutti gli Enti del territorio

Una volta accreditati, gli Enti della Constituency del **CSIRT di Regione Campania** potranno accedere immediatamente ai seguenti servizi offerti:

- **Portale web del CSIRT di Regione Campania**: il **CSIRT di Regione Campania** mette a disposizione un portale web ad accesso pubblico utilizzato per:
  - comunicare le proprie iniziative;
  - descrivere i servizi erogati;
  - pubblicare policy, linee guida e altri documenti prodotti a beneficio della Constituency;
  - emanare alert e bollettini di sicurezza.
  - In una II fase sarà realizzata un'area ad accesso riservato per: scambio di documenti tra CSIRT e singolo Ente, invio di segnalazioni al CSIRT da parte dell'Ente.
- **Iniziative di Training & Awareness**: il **CSIRT di Regione Campania** organizza eventi, online o in presenza, per finalità di formazione e sensibilizzazione su vari ambiti della sicurezza informatica rivolti al personale degli Enti della Constituency.
- **Report e alert di Cyber Threat Intelligence**: il **CSIRT di Regione Campania** fornisce report periodici e alert tempestivi (in caso di eventi che richiedono un trattamento immediato), contenenti informazioni utili per prevenire o mitigare attacchi informatici (quali vulnerabilità note su tecnologie, campagne di phishing, credenziali rubate, etc...) ottenute tramite attività di Cyber Threat Intelligence. Il servizio viene offerto su un numero limitato di asset per ciascun Ente (indicativamente 1 dominio e 1 subnet di indirizzi IP pubblici) – il quale dovrà essere comunicato al CSIRT per l'attivazione del servizio.

2.2. VALUTAZIONE MATURITÀ DEGLI ENTI CHE ADERISCONO ALL'INIZIATIVA

Allo scopo di valutare i livelli di maturità as-is e identificare aree di miglioramento in ambito di sicurezza informatica, il **CSIRT di Regione Campania** svolge opportuni **cyber maturity assessment** sugli Enti accreditati della Constituency. Questa attività si articola in diverse fasi chiave, ognuna delle quali è fondamentale per garantire un'analisi approfondita e mirata:

- ***Information Gathering e Set Up***, prevede la raccolta di informazioni preliminari necessarie per definire il perimetro dell'assessment. In questa fase, è essenziale identificare gli stakeholder interni all'Ente che possono fornire informazioni utili, raccogliere e censire la documentazione interna per analizzare lo stato attuale delle misure di sicurezza adottate, e mappare l'infrastruttura ICT per individuare gli asset critici, valutandone l'architettura;
- **Assessment** volto ad analizzare il contesto as-is degli Enti utilizzando una checklist «multicompliant», sviluppata in base ai principali controlli cyber previsti a livello nazionale e internazionale, come il NIST Cybersecurity Framework e il Framework ISO 27001;
- **Gap Analysis e Remediation** che comprende l'identificazione e l'analisi dei gap, individuando aree di non conformità rispetto agli standard internazionali. Sulla base del divario rilevato, il CSIRT, di concerto con l'Ente, definisce una roadmap di adeguamento, che prevede un piano d'azione dettagliato con la sequenza e la priorità degli interventi, inclusa l'implementazione di soluzioni quick-win per affrontare tempestivamente le vulnerabilità più critiche.

Le attività di **Cyber Maturity Assessment** hanno come obiettivo principale quello di fornire una visione chiara dello stato attuale delle misure di sicurezza adottate dagli Enti, identificare aree di miglioramento per innalzare il livello di maturità cyber, garantire la compliance con le normative e consolidare un piano strategico per la gestione della sicurezza, promuovendo una cultura della sicurezza e migliorando la resilienza complessiva della Constituency.

2.3. SERVIZI AD ATTIVAZIONE PROGRESSIVA

Di seguito sono riportati gli ulteriori servizi offerti dal **CSIRT di Regione Campania** cui gli Enti avranno la possibilità di accedere a seguito della loro progressiva attivazione.

- Il servizio di **Knowledge Transfer** permette al **CSIRT di Regione Campania** di condividere le proprie conoscenze e competenze con gli utenti dei membri della Constituency per aiutarli a riconoscere, prevenire e reagire alle minacce di sicurezza informatica. Tra gli obiettivi principali di questo servizio vi è la creazione di una **consapevolezza approfondita riguardo le diverse tipologie di minacce informatiche** che potrebbero influenzare la Constituency. Questo servizio si realizza attraverso un processo di formazione con lezioni, corsi ed esercitazioni pratiche volte a valutare e migliorare il livello di preparazione dei membri della Constituency.
- Il servizio di **Gestione delle Vulnerabilità** fornisce sostegno ai membri della Constituency del **CSIRT di Regione Campania** mediante l'identificazione, l'analisi e la gestione delle vulnerabilità, che siano ignote o conosciute. Tra gli **obiettivi principali perseguiti** dalle attività previste all'interno del servizio vi sono:
    - l'identificazione e l'analisi di vulnerabilità non ancora note;
    - la condivisione di informazioni riguardanti le nuove vulnerabilità scoperte;

- il supporto alla Constituency nel riconoscere e risolvere le vulnerabilità all'interno della propria infrastruttura.

- Il servizio di **Situational Awareness** è fondamentale per garantire la sicurezza informatica che si concentra sull'**analisi e l'interpretazione delle informazioni relative alle minacce cyber**. L'obiettivo principale del servizio è quello di fornire ai Membri della Constituency una visione del panorama delle minacce, permettendo loro di prepararsi e rispondere in modo efficace agli attacchi informatici. Il monitoraggio in ambito **Situational Awareness** si avvale di una combinazione di tecniche di analisi automatiche e manuali per raccogliere dati da una varietà di fonti, tra cui forum di hacker presenti sia sul clear web che sul dark web, database di vulnerabilità, report di incidenti e molto altro. Queste informazioni vengono poi analizzate per identificare **segnali di potenziali minacce** come campagne di phishing, exploit 0day e vulnerabilità non ancora note.
- Le attività di **Risposta agli Incidenti di Sicurezza** afferiscono al servizio di Gestione degli incidenti di sicurezza informatica. Nell'ambito di tali attività, il CSIRT di Regione Campania **supporta l'Ente della Constituency nell'analisi e comprensione dei dettagli relativi all'evento di sicurezza**, quali cause, sistemi impattati ed eventuali exploit utilizzati. Tra i principali obiettivi perseguiti dalle attività previste vi sono:
  - Supporto all'Ente per l'analisi e identificazione della causa alla base dell'incidente in corso di gestione;
  - Supporto all'Ente della Constituency nella definizione dei piani di rientro e mitigazione/ripristino dei sistemi impattati nell'incidente.
- I servizi di **Gestione degli Eventi e degli Incidenti di sicurezza informatica** comprendono:
  - Per la gestione degli **Eventi** (Information Security Event Management), il **CSIRT di Regione Campania** raccoglie, monitora e analizza gli eventi di sicurezza per identificare e qualificare potenziali incidenti. Questo include la gestione delle fonti di dati, il monitoraggio e l'analisi degli eventi, la correlazione degli eventi per ridurre i falsi positivi e l'identificazione di incidenti reali;
  - Per la gestione degli **Incidenti** (Information Security Incident Management), il CSIRT analizza, gestisce e dà supporto ai membri della Constituency nella mitigazione degli incidenti. Questo include l'analisi della causa degli incidenti, la raccolta e l'analisi delle evidenze, il supporto nella definizione dei piani di rientro, alla mitigazione e al ripristino dei sistemi impattati.

2.3.1. Modello di Delivery

Di seguito è descritto il **Modello di Delivery** per ciascun servizio ad attivazione progressiva:

Knowledge Transfer

- **Definizione dei Contenuti e dei Destinatari:** il CSIRT determina i contenuti dei corsi di formazione - assicurandosi che siano rilevanti e aggiornati rispetto alle minacce informatiche attuali - e i destinatari target all'interno dei membri della Constituency, specificando quali categorie di utenti necessitano della formazione (es. personale tecnico o tutta la popolazione aziendale)
- **Erogazione corso:** i corsi possono essere erogati secondo diverse modalità (sessioni frontali, in presenza o da remoto)
- **Condivisione Report:** il CSIRT condivide con l'ente un report dettagliato sui corsi erogati. Il report include il numero di utenti che hanno partecipato e completato con successo la formazione

Gestione delle Vulnerabilità

- **Svolgimento VA/PT:** il CSIRT esegue i VA/PT sui sistemi tramite l'utilizzo di strumenti automatizzati e tecniche manuali, al fine di identificare eventuali vulnerabilità
- **Condivisione del Report:** una volta completati i VAPT, il CSIRT prepara dei report dettagliati che vengono condivisi con la Constituency. I report contengono l'elenco delle vulnerabilità, una valutazione del rischio e delle raccomandazioni per la risoluzione delle vulnerabilità
- **Retest:** dopo che la Constituency ha implementato le correzioni, il CSIRT esegue dei retest sugli applicativi per verificare la corretta implementazione delle remediation
- **Condivisione del report finale:** il CSIRT condivide con la Constituency dei report contenente l'esito dei retest e dettagli su eventuali nuove vulnerabilità scoperte

Situational Awareness

- **Analisi di Data e Credential Leaks**: il CSIRT ricerca nel Clear, Deep e Dark Web informazioni per identificare potenziali leaks di documenti sensibili, credenziali, codici sorgente, domini di typosquatting e altri dump di informazioni;
- **Analisi del External Attack Surface**: il CSIRT ricerca su Internet i servizi pubblicamente accessibili ed esposti della Constituency (es. web app di produzione, database, server ftp, etc) e informazioni come indirizzi IP e la loro reputazione, record DNS che possono costituire un punto di ingresso per un threat actor esterno;
- **Analisi dei Social Media**: il CSIRT analizza i social media alla ricerca di informazioni, post e menzioni per valutare la reputazione da un punto di vista security, considerando tutte le informazioni pubblicamente disponibili;
- **Scenari di attacco potenziali**: i rischi considerabili come rilevanti vengono analizzati dal CSIRT sulla base delle analisi precedenti. Vengono definiti i potenziali casi d'uso che potrebbero

rappresentare un vettore d'attacco sfruttabile da un threat actor esterno per condurre un attacco mirato;

- **Reporting**: i risultati, le segnalazioni e le relative raccomandazioni vengono inviate sotto forma di report periodico o di segnalazione puntuale alla Constituency.

Risposta agli incidenti di sicurezza

- **Rilevamento e analisi:** a seguito della segnalazione da parte dell'Ente della Constituency, il CSIRT supporta l'organizzazione impattata nell'effettuare un triage iniziale e procedere con l'analisi dell'evento;
- **Contenimento ed eradication:** il CSIRT supporta l'Ente nell'avvio delle attività di contenimento sul ridurre al minimo l'impatto dell'incidente e sull'eliminazione della minaccia dagli asset impattati;
- **Ripristino:** il CSIRT, di concerto con l'Ente, individua le opportune azioni di rimedio per i sistemi impattati allo scopo di ripristinare l'operatività dei servizi e sistemi disabilitati;
- **Post-incident:** le azioni di risposta agli incidenti implementate dall'Ente vengono analizzate dal CSIRT con l'obiettivo di limitare la possibilità che l'incidente si ripeta ed identificare i modi per migliorare le future attività di risposta agli incidenti da parte della Constituency;
- **Reporting:** i risultati, le azioni di mitigazione e contenimento vengono opportunamente documentate e condivise con la Constituency e gli stakeholder rilevanti.

Gestione degli Eventi e degli Incidenti di Sicurezza

- **Configurazione delle fonti di dati e raccolta Log:** vengono identificati i sistemi da monitorare e configurate le sorgenti log affinché possano essere fornite come input al SIEM del CSIRT. I log possono essere raccolti da un collector configurato appositamente per inviarli al SIEM;
- **Monitoraggio degli Eventi e segnalazione degli incidenti di sicurezza:** l'analisi degli eventi generati dai log raccolti viene effettuata dal CSIRT. Qualora tali eventi dovessero essere catalogati come incidenti di sicurezza, verranno segnalati al Membro della Constituency interessato mediante i canali definiti;
- **Reporting:** a conclusione del processo, il CSIRT condivide il report contenente un riassunto delle informazioni raccolte durante l'intero processo di gestione dell'incidente.

2.3.2. Requisiti di Attivazione del Servizio

Di seguito sono riportati i requisiti di attivazione cui l'Ente richiedente è tenuto per l'attivazione di ciascun servizio. Nell'ambito di ciascun servizio, i I Membri della Constituency dovranno adempiere ai

seguenti requisiti di attivazione:

Knowledge Transfer
• Nel caso di sessioni frontali erogate in **presenza** indicare al CSIRT il numero di **utenti target** e **nominativi** che dovranno usufruire dei corsi di formazione; • Nel caso di sessioni frontali erogate da **remoto**, fornire quanto richiesto per le sessioni erogate in presenza e indicare l'indirizzo e-mail dei partecipanti.
Gestione delle Vulnerabilità
• **fornire al CSIRT tutte le informazioni rilevanti:** o sistemi da testare e rispettive URL; o eventuali credenziali necessarie; o eventuali VPN; o manleve firmate; • prendere in carico i report di VA/PT e procedere con la **risoluzione delle vulnerabilità** identificate
Situational Awareness
• **Fornire informazioni rilevanti** per mappare la superficie di attacco, come ad esempio: o nomi di dominio; o IP pubblici; o versione HW/SW dei dispositivi di sicurezza presenti sul perimetro (e.g. Cisco, Fortinet, ecc); o versione HW/SW dei dispositivi di rete ritenuti critici (e.g. vendor e modelli degli apparati di rete ecc..); o password policy applicate per le varie tipologie di utenze. • **Attuare le misure preventive consigliate** all'interno di ogni rispettivo report inviato dal CSIRT (es. reset credenziali, analisi degli asset citati nei report, controllo delle versioni software degli asset coinvolti, etc..)
Risposta agli incidenti di sicurezza
• **Comunicare i contatti di riferimento**: o Indirizzo email cifrato PGP; o Numero di telefono

- **Attuare le misure di mitigazioni individuate** all'interno di ogni rispettivo report inviato dal CSIRT (es. reset credenziali, analisi degli asset citati nei report, controllo delle versioni software degli asset coinvolti, etc..)

Gestione degli Eventi e degli Incidenti di Sicurezza

- **Configurare le sorgenti log** per l'invio al SIEM del CSIRT;
- **Comunicare i contatti di riferimento:**
    - Indirizzo email cifrato PGP;
    - Numero di telefono

2.4. ALLEGATI

2.4.1. Istanza di adesione al CSIRT di Regione Campania

Il sottoscritto:

Nome ……..

Cognome ……..

Codice Fiscale ……..

Funzione ……..

Tipologia Ente ……..

Ente ……..

Codice Fiscale dell'Ente ……..

Nella su qualità di legale rappresentante dell'ente o delegato (allegare delega o altra evidenza relativa alla legittimazione a rendere tale dichiarazione), consapevole delle pene stabilite per false attestazioni e dichiarazioni false o mendaci, giusta quando previsto dall'articolo 76 del D.P.R. n. 445/2000

dichiara

- di richiedere l'accreditamento dell'ente rappresentato al CSIRT di Regione Campania;
- che il referente in materia di sicurezza informatica è:

Nome ……..

Cognome ……..

Codice Fiscale ……..

Funzione ……..

Telefono ……..

Cellulare ……..

E-mail ……..

_____ _____

Data e Luogo **Firma**

2.4.2. Selezione Servizi

Di seguito sono elencati i servizi offerti dal **CSIRT di Regione Campania**. È prevista la fornitura di tutti i servizi disponibili in modo integrato. Pertanto, nel caso in cui si verifichino eventuali eccezioni, ad esempio qualora l'Ente disponga già di un servizio specifico, si prega di segnalare la motivazione per l'eventuale eccezione nelle note aggiuntive. Questo consentirà al **CSIRT di Regione Campania** di garantire un servizio personalizzato e adeguato alle esigenze di ciascun Ente della Constituency.

- □ **Knowledge Transfer**

Note: _____

- □ **Gestione delle Vulnerabilità**

Note: _____

- □ **Situational Awareness**

Note: _____

- □ **Risposta agli incidenti di sicurezza**

Note: _____

- □ **Gestione degli Eventi e degli Incidenti di Sicurezza**

Note: _____

_____ _____

Data e Luogo **Firma**

Allegato B

ATTO DI NOMINA

A RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

ai sensi dell'art. 28 del Regolamento UE 2016/679 del 27 aprile 2016

tra

REGIONE CAMPANIA – UFFICIO SPECIALE PER LA CRESCITA E LA TRANSIZIONE DIGITALE (C.F. 80011990639), con sede legale in Napoli, Via Don Bosco, n. 9/F, rappresentato dal Direttore Generale, Dott. Massimo Bisogno, domiciliato presso la sede, in ragione della carica ed agli effetti del presente atto,

(di seguito, anche «**U.S. 11**»)

e

P.A(C.F. ……) con sede legale in Napoli, ……., rappresentata del Direttore Generale, Dott._____, domiciliato presso la sede, in ragione della carica ed agli effetti del presente accordo, di seguito anche Fruitore

(di seguito, anche «**P.A.L.**» o «**Fruitore**»)

(di seguito, congiuntamente denominati anche le «**Parti**»)

PREMESSO CHE

a) la Cybersecurity è uno dei sette investimenti della Digitalizzazione della pubblica amministrazione, primo asse di intervento della componente 1 "Digitalizzazione, innovazione e sicurezza nella PA" compresa nella Missione 1 "Digitalizzazione, innovazione, competitività, cultura e turismo" del PNRR;
b) in data 11/08/2023 l'Agenzia per la cybersicurezza nazionale, in qualità di Soggetto attuatore, ha pubblicato l'avviso pubblico a sportello per la presentazione di proposte di interventi volti all'attivazione e al potenziamento di CSIRT Regionali, ossia di strutture di "Computer Security Incident Response Team" incardinati presso le Amministrazioni regionali, per il rafforzamento delle capacità di prevenzione, gestione e risposta degli incidenti informatici, nell'ambito della Missione 1 Componete 1 – Investimento 1.5 "Cybersecurity" – Codice d'investimento M1C1I1.5 del PNRR finalizzato a contribuire all'attuazione di investimenti finalizzati al rafforzamento delle capacità tecniche nazionali in materia di prevenzione e risoluzione di incidenti cyber, mediante l'attivazione di squadre di pronto intervento informatico deputate alla gestione degli incidenti e degli attacchi informatici sui propri sistemi informativi;
c) l'avviso è destinato a finanziare, mediante procedura a sportello, per un valore complessivo di 28M€ – secondo l'ordine cronologico di presentazione delle Istanze di partecipazione e fino alla concorrenza delle risorse disponibili – progettualità cd. a regia volte all'attivazione o al potenziamento di Computer Security Incident Response Team (CSIRT) da costituirsi o già costituiti presso le Regioni e le Province autonome, coerentemente con i requisiti minimi individuati dalle "Linee Guida per la realizzazione di uno CSIRT";
d) con Delibera di Giunta Regionale n. 537 del 22/09/2023 è stato disposto di aderire all'Avviso Pubblico del 11/08/2023 dell'Agenzia per la cybersicurezza nazionale per la presentazione di proposte di interventi volti all'attivazione e al potenziamento di CSIRT Regionali per il rafforzamento delle capacità di

prevenzione, gestione e risposta degli incidenti informatici, a valere sul PNRR, Missione 1 Componete 1 – Investimento 1.5 "Cybersecurity" – Codice d'investimento M1C1I1.5;

e) in data 30 novembre 2023 (prot.n. 0030697.30-11-2023.I) è stata firmata dal Direttore Generale dell'Agenzia di Cybersicurezza Nazionale la determina avente ad oggetto "Avviso Pubblico n. 06/2023 recante "Avviso Pubblico a sportello per la presentazione di proposte di interventi volti all'attivazione e al potenziamento di CSIRT Regionali per il rafforzamento delle capacità di prevenzione, gestione e risposta degli incidenti informatici PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 – Componente 1 –Investimento 1.5 "Cybersecurity"M1C1I1.5". Determina di concessione del finanziamento e contestuale rifinanziamento e approvazione della graduatoria finale e di destinazione delle risorse;

f) con la suddetta determina sono stati approvati la graduatoria definitiva a valere sull'Avviso 6/2023 e i relativi allegati: (Allegato A) graduatoria definitiva delle proposte progettuali ammesse e totalmente finanziabili, (Allegato B) graduatoria definitiva proposte progettuali ammesse e parzialmente finanziabili, (Allegato C) graduatoria definitiva proposte progettuali idonee ma non finanziabili, (Allegato D) elenco delle proposte progettuali non ammesse";

g) la proposta progettuale "CSIRT Campania" della Regione Campania è risultata tra le proposte ammesse e totalmente finanziabili per un importo complessivo pari ad € 1.499.904,60;

h) con la Delibera di Giunta Regionale n. 551 del 24 ottobre 2024, è stato disposto:

- di istituire il Computer Security Incident Response Team (CSIRT) della Regione Campania demandando all'Ufficio speciale per la crescita e la transizione digitale, anche in qualità di RTD dell'Ente, tutti gli adempimenti necessari per l'attivazione del CSIRT nonché, le modalità di integrazione per lo svolgimento delle funzioni regionali assegnate in qualità di Autorità di settore dalla disciplina NIS;
- di stabilire che il CSIRT, in fase di avvio, svolga la propria attività con riferimento alle strutture della Regione Campania, con possibilità futura di integrare ed ampliare la realizzazione di un servizio a supporto del territorio nella prevenzione e risposta agli incidenti di sicurezza informatica, operando in un'ottica di filiera, con tutti gli Enti del territorio regionale;
- di demandare all'Ufficio speciale per la crescita e la transizione digitale l'individuazione della struttura di governo, le tecnologie, la precisazione dei servizi inclusi nella soluzione di CERT Regionale, dei ruoli e delle tempistiche di attuazione, la definizione della constituency, delle competenze e professionalità, delle responsabilità e modalità di funzionamento del modello organizzativo, dei processi di attivazione e coordinamento per la gestione di eventuali incidenti di sicurezza, delle regola e dei costi di gestione annuali, dei modelli di adesione e di partecipazione alla spesa;

i) le Parti hanno ravvisato il reciproco interesse finalizzato al perseguimento dei relativi obiettivi istituzionali ad attivare le necessarie forme di cooperazione per la piena attuazione delle attività demandate dalla D.G.R. n. 551/2024, con l'articolazione e la pianificazione delle azioni, i tempi di esecuzione delle rispettive attività e l'impiego delle rispettive risorse e di ogni conseguente adempimento amministrativo;

j) in data […], le Parti hanno dunque sottoscritto l'accordo di cooperazione orizzontale, ai sensi dell'art. 15 della Legge 7 agosto 1990, n. 241 e dell'art. 7, comma 4, del D.Lgs. 31 marzo 2023 n. 36 (di seguito, anche «**Accordo**»), finalizzato a disciplinare i rapporti di cooperazione istituzionale tra l'U.S. 11 e gli Enti

Fruitori, in attuazione della D.G.R. n. 551 del 24 ottobre 2024, per la realizzazione delle attività connesse all'istituzione e al funzionamento del Computer Security Incident Response Team (CSIRT) della Regione Campania.;

k) per le finalità connesse e strumentali all'adempimento delle prestazioni oggetto dell'Accordo, l'Ente Fruitore potrà venire a conoscenza e/o acquisire dati e informazioni personali e/o riservate di titolarità della Regione;

l) in relazione ai dati e alle informazioni trattati nell'ambito dell'Accordo, la Regione, per quanto di propria competenza, è titolare del trattamento dei dati personali (di seguito, anche «**Titolare**») e, con il presente Atto intende pertanto nominare il Fruitore quale responsabile del trattamento dei dati personali (di seguito, anche «**Responsabile**»), ai sensi dell'art. 28 del GDPR;

SI STIPULA E SI CONVIENE QUANTO SEGUE:

1. La Regione Campania nomina il Fruitore, che accetta, Responsabile del trattamento dei dati personali di cui in premessa, affidando i seguenti compiti ed impartendo le seguenti istruzioni per il trattamento dei dati, ai fini dello svolgimento delle attività oggetto dell'Accordo:

a) effettuare i trattamenti di dati personali indispensabili e strumentali alle finalità di cui sopra, attenendosi alle prescrizioni contenute nel presente Atto, nel GDPR, e, in generale, nella normativa in materia di protezione dei dati personali, nonché alle eventuali successive istruzioni che potranno essere impartite dal Titolare;

b) adottare e rispettare le misure di sicurezza adeguate al livello di rischio del trattamento di cui agli artt. 32 e ss. del GDPR, al fine di assicurare i principi di integrità e riservatezza dei dati personali trattati, evitando trattamenti non autorizzati e/o illeciti oltre a qualsiasi forma di perdita o distruzione, anche accidentale dei dati;

c) ai sensi dell'art. 30 del GDPR, e nei limiti di quanto esso prescrive, tenere un Registro delle attività di trattamento effettuate sotto la propria responsabilità e cooperare con il Titolare del trattamento e con l'Autorità Garante per la protezione dei dati personali, mettendo il predetto Registro a disposizione del Titolare del trattamento e dell'Autorità, laddove ne venga fatta richiesta ai sensi dell'art. 30, comma 4, del GDPR;

d) informare senza ingiustificato ritardo il Titolare del trattamento di ogni eventuale violazione dei dati personali subita in relazione ai trattamenti dei dati svolti per conto dello stesso e fornire al titolare, entro comunque 24 ore dalla scoperta della violazione, ogni elemento utile in suo possesso al fine di consentire al Titolare medesimo le necessarie valutazioni;

e) assistere il Titolare, su richiesta dello stesso e laddove ciò sia possibile, anche con misure tecniche e organizzative adeguate, nel dare seguito alle richieste per l'esercizio dei diritti dell'interessato, come previsto agli artt. 15 e ss. del GDPR;

f) nominare, autorizzare e impartire istruzioni scritte ai soggetti autorizzati (di seguito anche «**Soggetto Autorizzato**» o «**Autorizzato**») a svolgere le attività di trattamento riconducibili a quanto previsto dal presente Atto, affinché gli stessi siano in condizione di porre in essere esclusivamente quelle operazioni di trattamento che siano assolutamente necessarie e strumentali, facendo fin d'ora divieto ai medesimi,

salvo specifica autorizzazione scritta dal Titolare del trattamento, di procedere alla diffusione, comunicazione, distruzione, cancellazione, modifica, raffronto, incrocio, eliminazione e in genere a qualsiasi operazione che non sia volta per volta consentita o che non sia strettamente connessa agli adempimenti previsti dall'Accordo, dal presente Atto o dalla normativa di settore;

g) secondo le indicazioni fornite per iscritto dal Titolare del trattamento, restituire al Titolare medesimo o distruggere i dati personali alla fine del trattamento degli stessi. Nei casi previsti dalla normativa, d'accordo con il Titolare, l'Ente Fruitore avrà facoltà di mantenere almeno una copia dei dati trattati al fine di assolvere ad obblighi legali di conservazione e rispettare le proprie procedure in tema di documentazione dell'attività svolta (ad esempio per richiesta di un'Autorità o in caso di contenzioso di qualsivoglia natura);

h) prestare la propria collaborazione in caso di eventuali richieste dell'Autorità Garante per la Protezione dei Dati Personali o dell'Autorità Giudiziaria, pervenute a qualunque titolo al Titolare e inerenti ai trattamenti oggetto del presente Atto, per fornire al Titolare medesimo tutte le informazioni necessarie per soddisfare le interrogazioni delle Autorità;

i) informare tempestivamente, se normativamente consentito, il Titolare, nel caso in cui sia diretto destinatario di richieste dell'Autorità Garante per la Protezione dei Dati Personali o dell'Autorità giudiziaria o di ispezioni ed a collaborare per gli interventi opportuni ed eventualmente necessari;

j) salvo diversa pattuizione con il Titolare del trattamento, trattare i dati esclusivamente all'interno dell'Unione Europea/Spazio Economico Europeo;

k) ove necessario in relazione alle prestazioni di cui all'Accordo, formare, nominare, autorizzare ed impartire istruzioni scritte agli amministratori di sistema assegnati a svolgere le attività di trattamento riconducibili a quanto previsto dal presente Atto, nonché vigilare sul rispetto delle suddette istruzioni;

l) accettare che il Titolare del trattamento si riservi la facoltà, anche tramite verifiche periodiche, di vigilare sulla puntuale osservanza delle predette disposizioni e delle proprie istruzioni, anche affidando l'incarico a consulenti esterni contrattualmente sottoposti a vincoli di riservatezza e confidenzialità.

2. La presente nomina a Responsabile è efficace a far data dal conferimento dell'incarico mediante sottoscrizione dell'Accordo e avrà durata pari a quella dell'Accordo medesimo. Nel caso in cui l'Accordo dovesse essere oggetto di estensione, si estenderà tacitamente anche la durata del presente Atto. Alla scadenza dell'Accordo, ovvero qualora il rapporto tra le Parti venisse meno o perdesse efficacia per qualsiasi motivo, anche il presente Atto decadrà automaticamente senza bisogno di comunicazioni o revoche e l'Ente Fruitore non sarà più legittimato a trattare i dati della Regione Campania.

3. Per tutto quanto non previsto dal presente Atto di nomina, si rinvia alle disposizioni generali vigenti ed applicabili in materia di protezione dei dati personali.

4. Tutte le comunicazioni previste dal presente atto di nomina, nonché in generale ogni comunicazione in materia di tutela dei dati personali, dovrà essere effettuata mediante posta elettronica certificata:

- quanto al Titolare del trattamento, Regione Campania, casella PEC […];
- quanto al Responsabile del trattamento dei dati personali, P.A:, casella PEC […].

5. Il presente Atto è stato oggetto di puntuale negoziazione tra le Parti, con la conseguenza che non si rende necessaria l'accettazione specifica di clausole del medesimo ai sensi degli artt. 1341 e 1342 c.c.

6. Le premesse in epigrafe e gli allegati al presente Atto formano parte integrante e sostanziale dello stesso.

Letto, confermato e sottoscritto con firme digitali.

Napoli, [...] 2025.

REGIONE CAMPANIA – UFFICIO SPECIALE PER LA CRESCITA E LA TRANSIZIONE DIGITALE
Il Direttore Generale
Dott. MASSIMO BISOGNO

ENTE FRUITORE.
Il Direttore
DOTT. _____

ISTRUZIONI PER IL TRATTAMENTO DEI DATI PERSONALI

Il Responsabile, nell'ambito delle attività connesse all'istituzione e al funzionamento del Computer Security Incident Response Team (CSIRT) della Regione Campania, dovrà rispettare le *best practices* internazionali e nazionali di settore, nonché eventuali misure di salvaguardia disposte dal Garante per la protezione dei dati personali, e garantire al contempo il rispetto della normativa in materia di digitalizzazione e cybersicurezza (ad es., CAD e Linee Guida AGID, Linee Guida ACN), quali, ad esempio, le «*Linee Guida AGID sulla formazione, gestione e conservazione dei documenti informatici*» di settembre 2020/maggio 2021, la Determinazione AGID n. 628/2021 del 15 dicembre 2021 in materia di «*Cloud della PA*», il Provvedimento del Garante n. 393 del 2 luglio 2015, in materia di «*Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche*», le Linee Guida di ACN del 26 novembre 2024 «*Per il rafforzamento della protezione delle banche dati rispetto al rischio di utilizzo improprio*».

La Regione Campania, in qualità di Titolare del trattamento dei dati personali, potrà fornire in un momento successivo istruzioni specifiche di carattere tecnico/informatico cui l'Ente fruitore dovrà necessariamente attenersi.

Il Responsabile, nell'ambito delle operazioni di trattamento necessarie per l'espletamento dell'Accordo, dovrà rispettare in ogni caso le seguenti misure:

1) rispettare gli obblighi di riservatezza e segretezza e, conseguentemente, il divieto di comunicazione e diffusione dei dati personali trattati a terzi non autorizzati;

2) installare sugli elaboratori idonei programmi contro il rischio di intrusione e accesso abusivo, da aggiornare periodicamente ed in occasione di ogni versione disponibile dalla casa madre;

3) provvedere, ogni qualvolta vi sia la segnalazione della presenza di vulnerabilità nei programmi utilizzati e la contemporanea disponibilità delle opportune modifiche, all'aggiornamento, entro un congruo periodo di tempo, dei programmi utilizzati, o almeno alla valutazione degli impatti sull'aggiornamento;

4) individuare per iscritto i Soggetti Autorizzati al trattamento dei dati personali, ai sensi dell'art. 2-*quaterdecies* del D.Lgs. 196/2003, impartendo agli stessi le istruzioni idonee alle attività da svolgere;

5) garantire che l'accesso a tali dati personali sia effettuato unicamente da soggetti a ciò abilitati in ragione delle funzioni professionali svolte dagli stessi;

6) prevedere che i Soggetti Autorizzati possano porre in essere solo le attività assolutamente necessarie e strumentali all'esecuzione dell'Accordo, con divieto nei confronti degli stessi, salvo specifica autorizzazione scritta dal Titolare del trattamento, di procedere alla diffusione, comunicazione, distruzione, cancellazione, modifica, raffronto, incrocio, eliminazione e in genere a qualsiasi operazione che non sia volta per volta consentita o che non sia strettamente connessa agli adempimenti previsti dall'Accordo, dal presente Atto o dalla normativa di settore;

7) prevedere che il trattamento dei dati personali possa avvenire solo mediante dispositivi aziendali forniti dal Fruitore, protetti da adeguate ed efficaci credenziali di autenticazione. Le credenziali di autenticazione consistono in un codice per l'identificazione del soggetto autorizzato al trattamento associato a una parola chiave riservata conosciuta solamente dal medesimo, oppure in un dispositivo di autenticazione in possesso e uso esclusivo del soggetto autorizzato al trattamento, eventualmente associato a un codice identificativo o a una parola chiave;

8) prescrivere le necessarie cautele per assicurare la segretezza delle suddette credenziali di autenticazione e/o la diligente custodia del dispositivo in possesso ed uso esclusivo del soggetto autorizzato al

trattamento;

9) assicurare che il trattamento da parte di ciascun Soggetto Autorizzato sarà effettuato per il solo tempo necessario al compimento delle operazioni allo stesso assegnate ai fini dell'esecuzione dell'Accordo;

10) vietare ai Soggetti Autorizzati di porre in essere azioni che possano causare l'introduzione nei dispositivi di virus;

11) prevedere che, in caso di allontanamento dell'autorizzato dalla postazione di lavoro, l'autorizzato medesimo dovrà evitare che vi sia possibilità da parte di terzi (anche se colleghi o comunque appartenenti alla struttura) di accedere ai dati personali per i quali sia in corso una qualunque operazione di trattamento, sia essa mediante supporto cartaceo o informatico;

12) ove necessario in relazione alle prestazioni di cui all'Accordo, redigere e mantenere aggiornato un elenco con gli estremi identificativi delle persone fisiche che rivestono il ruolo di Amministratori di Sistema e, per ciascuno di essi, la descrizione delle funzioni che gli sono state attribuite nell'ambito delle attività svolte per conto del Titolare del trattamento e implementare le ulteriori Misure di sicurezza, come definito nel Provvedimento dell'Autorità Garante per la Protezione dei dati personali del 27 novembre 2008, recante "*Misure e accorgimenti prescritti al Titolare dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratori di sistema*";

13) garantire il pieno coordinamento con gli altri soggetti coinvolti nel trattamento dei dati personali – quali, ad esempio, Regione, Aziende Sanitarie, Operatori e Strutture sanitarie – proponendo misure tecnico-giuridiche finalizzare alla integrazione e alla sinergia con gli stessi (ad es., procedure, protocolli operativi);

14) garantire il rispetto della *data protection* nell'ambito dell'intero ciclo di vita dei dati personali, anche mediante misure tecnico-organizzative differenziate a seconda del soggetto di volta in volta coinvolto (ad es., MMG/PLS, Medico Specialista, ecc.);

15) adottare misure per l'acquisizione e la conservazione dei consensi (ove necessari in ragione degli specifici trattamenti, alla luce dei "*Chiarimenti sull'applicazione della disicplina per il trattamento dei dati relativi alla salute in ambito sanitario*" resi dal Garante per la protezione dei dati personali in data 7 marzo 2019) nel rispetto del GDPR (i.e., art. 7) e delle prassi UE e nazionali.

In merito al trattamento dei dati personali con strumenti diversi da quelli elettronici, il Responsabile è tenuto a:

- predisporre un archivio per gli atti ed i documenti con dati personali, individuando per iscritto i Soggetti Autorizzati al trattamento con i relativi profili di accesso ai dati ed ai documenti;
- definire procedure di deposito, custodia, consegna o restituzione e compartimentazione dei dati stessi (ad esempio, un registro e degli armadi separati e chiusi).

Il Responsabile potrà ricorrere ad un altro Responsabile del trattamento (di seguito, "***Sub-Responsabile del trattamento***") per delegargli attività di trattamento specifiche, previa autorizzazione scritta del Titolare del trattamento. I Sub-Responsabili dovranno essere nominati tramite contratto o atto giuridico avente ad oggetto i medesimi obblighi imposti al Responsabile con il presente Atto di nomina e, in particolare, nel rispetto delle condizioni di cui ai paragrafi 2 e 4 dell'art. 28 del GDPR. In caso di mancato adempimento da parte del Sub-Responsabile del trattamento degli obblighi in materia di protezione dei dati, il Responsabile iniziale del trattamento è interamente responsabile nei confronti del Titolare del trattamento di tali inadempimenti; la Regione potrà in qualsiasi momento verificare le garanzie e le misure tecniche ed organizzative del Sub-Responsabili, tramite audit e ispezioni anche avvalendosi di soggetti terzi non concorrenti del Responsabile. In caso di nomina di Sub-Responsabili, il Responsabile risponderà, nei confronti del Titolare, dei relativi inadempimenti a meno che non riesca a dimostrare che il danno non è in alcun modo a lui imputabile.

Il Responsabile è chiamato ad evadere tempestivamente le richieste del Titolare e a collaborare con lo stesso all'adozione di soluzioni organizzative, logistiche, tecniche e procedurali idonee ad assicurare l'osservanza delle disposizioni vigenti in materia di trattamento dei dati personali.

Il Responsabile è inoltre chiamato a collaborare con il Titolare al fine di consentire a quest'ultimo di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui agli articoli da 15 a 22 del GDPR.