AZIENDA OSPEDALIERA UNIVERSITARIA

DELIBERA DEL COMMISSARIO STRAORDINARIO

Deliberazione n. 1504 del 21/11/2023

OGGETTO: stipula del Protocollo d'Intesa tra la Polizia di Stato – Centro Operativo Sicurezza Cibernetica -Polizia Postale e delle Comunicazioni e questa Azienda Ospedaliero Universitaria Policlinico "Paolo Giaccone" (AOUP), finalizzato a regolamentare le attività di prevenzione e contrasto dei crimini informativi su sistemi informativi "critici" di supporto alle funzionali istituzionali dell' AOUP, validità triennale a far data dalla sottoscrizione.

STRUTTURA PROPONENTE **AREA AFFARI GENERALI** **Proposta n. 134 del 13/11/2023** L'estensore dell'atto **Dott.ssa Antonella Pastore** Il Responsabile del Procedimento **Cinzia Di Noto** Il Responsabile dell'UOS Relazioni Istituzionali, Convenzioni, Gestione Documenti e Sinistri. **Dott. Francesco Palma** Il Direttore dell'UOC **Dott. Vincenzo Manzella**	**Area Gestione Economico - Finanziaria** Autorizzazione spesa n. _____ del _____ Conto di costo _____ NULLA OSTA in quanto conforme alle norme di contabilità **Il Responsabile dell'Area Economico–Finanziaria e Patrimoniale** **Dott. Luigi Guadagnino** ☐ **Non comporta ordine di spesa**

Ai sensi del DPR n. 445/2000 e ss.mm.ii., della Legge n. 241/90 e ss.mm.ii.e della L.R. 7/2019, il sottoscritto attesta la regolarità della procedura seguita e la legalità del presente atto, nonché l'esistenza della documentazione citata e la sua rispondenza ai contenuti esposti.
Il Responsabile dell'Unità proponente: Dott. Vincenzo Manzella

L'anno duemilaventitre, il giorno 21 del mese di NOVEMBRE, nei locali della sede legale di Via del Vespro 129, Palermo, il Commissario Straordinario dell'Azienda Ospedaliera Universitaria Policlinico "Paolo Giaccone" di Palermo, Dott. Maurizio Montalbano, nominato con D.A. n.28 del 29 giugno 2023 e prorogato con D.A n. 32 del 27 Ottobre 2023, assistito dalla DOTTSSA GABRIELLA DONZELLI, quale segretario verbalizzante, adotta la seguente delibera sulla base della proposta di seguito riportata.

AZIENDA OSPEDALIERA UNIVERSITARIA

IL DIRETTORE DELL'UOC AFFARI GENERALI

Dott. Vincenzo Manzella

VISTO il D. Lgs. del 30/12/1992 n. 502, recante "Riordino della disciplina in materia sanitaria" a norma dell'art. 1 della Legge 23 ottobre 1992 n. 421, e ss.mm.ii.;

VISTO il D. Lgs. del 21 dicembre 1999, n. 517 che disciplina i rapporti tra il Servizio Sanitario Nazionale e le Università a norma dell'art. 6 della legge 30 novembre 1998 n. 419;

VISTO il D. Lgs. 30 giugno 2003 n. 196 "Codice in materia di protezione del dati personali" e ss.mm.ii.;

VISTA la Legge regionale n. 5 del 14 aprile 2009 pubblicata nella G.U.R.S. parte I n. 17 del 17aprile 2009, con la quale si stabiliscono le norme per il riordino del Servizio Sanitario Regionale, in conformità ai principi contenuti nel decreto legislativo 30 dicembre 1992 n. 502 e ss.mm.ii;

VISTO il Protocollo di intesa, stipulato tra la Regione Siciliana – Assessorato della Sanità, e l'Università di Palermo del 10 marzo 2020 pubblicati nella GURS n. 19 del 3 aprile 2020, in atto vigente.

PREMESSO

che l'articolo 39 della legge 16 gennaio 2003, n. 3, recante: *"Disposizioni ordinamentali in materia di pubblica amministrazione"* prevede che il Dipartimento della Pubblica Sicurezza, nell'ambito delle direttive impartite dal Ministro dell'Interno per il potenziamento dell'attività di prevenzione, può stipulare convenzioni con soggetti, pubblici e privati, dirette a fornire, con la contribuzione degli stessi soggetti, servizi specialistici, finalizzati ad incrementare la sicurezza pubblica;

che il decreto legge 27 luglio 2005 n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005 n. 155, recante *"Misure urgenti per il contrasto del terrorismo internazionale"*, ed in particolare l'art. 7 bis, comma 1, dispone che con decreto del Ministro dell'Interno siano individuate le infrastrutture critiche informatizzate di interesse nazionale, alla cui protezione informatica provvede l'organo del Ministero dell'Interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, operando mediante collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture interessate;

che la Direttiva del Ministro dell'Interno del 15 agosto 2017 "sui comparti delle Specialità e sulla razionalizzazione dei Presidi di Polizia" ha ribadito al punto 1.4 la competenza della Polizia Postale e delle Comunicazioni in materia di protezione delle infrastrutture critiche nonché di sicurezza e regolarità dei servizi di telecomunicazione;

che nell'ambito della direttiva generale per l'attività amministrativa e per la gestione relativa all'anno 2023, il Ministro dell'Interno, in ordine agli obiettivi operativi, nel ribadire l'esigenza di tutelare dalle minacce cyber coloro che operano nel mondo della rete, anche attraverso appositi contatti bilaterali (intese, riunioni, accordi, ecc.) tra l'amministrazione e gli enti gestori di sistemi e servizi strategici, ha altresì previsto il rafforzamento – attraverso le risorse del PNRR – delle difese cibernetiche, aumentando il grado di resilienza informatica dell'amministrazione attraverso la creazione di sezioni operative per la sicurezza cibernetica distrettuali, di laboratori operativi dotati delle infrastrutture per le attività forensi (CLABS) e il potenziamento della sala server, al fine di prevedere o rilevare tempestivamente attacchi e incidenti informatici;

che, con decreto del Capo della Polizia del 28 giugno 2022, è stata attuata la complessiva revisione dell'assetto ordinativo delle articolazioni periferiche dell'Amministrazione della Pubblica Sicurezza e, in particolare, dei Centri Operativi per la Sicurezza Cibernetica (C.O.S.C.) quale nuova denominazione dei Compartimenti di Polizia Postale e delle Comunicazioni, al cui interno sono stati istituiti i Nuclei Operativi Sicurezza Cibernetica (N.O.S.C.);

che con il D.Lgs. 18 maggio 2018 n. 65 è stata recepita la 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"* (c.d. Direttiva NIS), che individua quale Autorità di contrasto il Servizio Polizia Postale e delle Comunicazioni in qualità di organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, di cui all'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n.155, così come individuato dal Decreto Interministeriale del 10 gennaio 1999;

che il Centro Operativo Sicurezza Cibernetica - Polizia Postale e delle Comunicazioni Sicilia Occidentale (*di seguito denominato brevemente Centro*) provvede, come organo periferico del Servizio Polizia Postale e delle Comunicazioni del Dipartimento della Pubblica Sicurezza, ad assicurare i Servizi della Polizia Postale e delle Comunicazioni, con particolare riferimento alla prevenzione e repressione dei reati commessi avvalendosi delle specifiche potenzialità tecniche dei servizi o mezzi di comunicazione, anche ad alta tecnologia, ovvero alterando il normale funzionamento degli stessi;

ATTESO

che i sistemi informatici e le reti telematiche di supporto alle funzioni istituzionali di questa Azienda Ospedaliera Universitaria Policlinico "Paolo Giaccone" (*di seguito brevemente AOUP*) sono da considerare infrastrutture sensibili di interesse pubblico;

che la cooperazione tra il Centro e questa AOUP è volta alla prevenzione e alla repressione dei crimini informatici, ispirata al principio di sicurezza partecipata, mira alla condivisione di specifiche procedure d'intervento, che potranno essere declinate in appositi modelli operativi di collaborazione per il contrasto degli attacchi informatici.

CONSIDERATO CHE

il Centro, con nota prot.0014845 del 11.09.2023, introitata al prot. gen.le di questa AOUP in pari data al n. 56332, a conclusione di specifici incontri con il Responsabile del Servizio Informativo Aziendale dell'AOUP ha rappresentato la propria disponibilità al perfezionamento di un Protocollo d'Intesa volto a disciplinare la collaborazione in parola.

RAVVISATA l'opportunità, per le ragioni sopra esposte, di procedere all'attivazione dei rapporti giuridici in parola derivanti dall'attuazione degli accordi, degli atti presupposti connessi e/o consequenziali.

STABILITO

dalle parti contraenti di formalizzare detti rapporti mediante la sottoscrizione di un Protocollo d'Intesa, costituito da nr 6 pagine, 7 articoli che, allegato, costituisce parte integrante e sostanziale del presente atto.

che le attività in narrativa verranno assicurate dal Centro in collaborazione con l'U.O. Sistemi Informativi Aziendali (SIA) dell'AOUP.

la validità dello stesso è pari ad anni tre a far data dal suo perfezionamento.

PRESO ATTO CHE:

con nota inviata a mezzo mail in data 13.11.2023 il Responsabile del U.O. Sistemi Informativi Aziendali in risposta alla precisa richiesta dell'Ufficio Convenzioni ha dichiarato che non vi sono spese per le esigenze di cybersecurity in atto presumibili per il rafforzamento delle infrastrutture di rete;

il Protocollo d'Intesa si propone le seguenti finalità dalle quali discendono gli obblighi delle parti connessi alla loro attuazione:

- la condivisione e l'analisi di informazioni idonee a prevenire e contrastare attacchi o danneggiamenti in pregiudizio delle infrastrutture informatiche per le finalità di contrasto dei crimini informatici;
- la segnalazione di emergenze relative a vulnerabilità, minacce ed incidenti in danno della regolarità dei servizi di telecomunicazione;
- l'identificazione dell'origine degli attacchi che abbiano come destinazione le infrastrutture tecnologiche gestite da o che traggano origine dalle medesime;
- alla realizzazione e alla gestione di attività di comunicazione fra le Parti per fronteggiare situazioni di emergenza.

DATO ATTO che il Direttore dell'UOC AFFARI GENERALI che propone il presente provvedimento, sottoscrivendolo, attesta che lo stesso, a seguito dell'istruttoria effettuata e' conforme alla normativa che disciplina la materia trattata ed è, sia nella forma che nella sostanza, totalmente legittima, veritiero e utile per il servizio pubblico, ai sensi e per gli effetti di quanto disposto dall'art. 1 della L. 14 gennaio 1994 n. 20 e succ. modifiche ed integrazioni, e che lo stesso e' stato predisposto nel rispetto della legge 6 novembre 1990 n. 190 "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella Pubblica Amministrazione" nonché nell'osservanza dei contenuti del vigente Piano Aziendale della Prevenzione della Corruzione.

PROPONE DI

di stipulare il Protocollo d'Intesa tra la Polizia di Stato – Centro Operativo Sicurezza Cibernetica -Polizia Postale e delle Comunicazioni e questa Azienda Ospedaliero Universitaria Policlinico "Paolo Giaccone" (AOUP), finalizzato a regolamentare le attività di prevenzione e contrasto dei crimini informativi su sistemi informativi "critici" di supporto alle funzionali istituzionali dell'AOUP.

di approvare lo schema di protocollo, recante la regolamentazione dei rapporti giuridici ed economici statuiti tra le Parti costituito da n. 6 pagine, 7 articoli che, allegato, costituisce parte integrante e sostanziale del presente provvedimento

di stabilire che:

le attività in narrativa verranno assicurate dal Centro in collaborazione con l'U.O. Sistemi Informativi Aziendali (SIA) dell'AOUP.

la validità dello stesso è pari ad anni tre a far data dal suo perfezionamento.

di prendere atto che:

il Protocollo d'Intesa si propone le seguenti finalità dalle quali discendono gli obblighi delle parti connessi alla loro attuazione:

- la condivisione e l'analisi di informazioni idonee a prevenire e contrastare attacchi o danneggiamenti in pregiudizio delle infrastrutture informatiche per le finalità di contrasto dei crimini informatici;
- la segnalazione di emergenze relative a vulnerabilità, minacce ed incidenti in danno della regolarità dei servizi di telecomunicazione;
- l'identificazione dell'origine degli attacchi che abbiano come destinazione le infrastrutture tecnologiche gestite da o che traggano origine dalle medesime;
- la realizzazione e alla gestione di attività di comunicazione fra le Parti per fronteggiare situazioni di emergenza.

di munire il presente provvedimento di immediata esecutività, ai sensi e per gli effetti di quanto disposto dall'art. 53 comma 7 Legge regionale 30/93, al fine di non procrastinare oltre le attività oggetto del Protocollo d'Intesa.

di notificare al Responsabile dei Sistemi Informativi Aziendali, al DPO, nonché al Resp.le del Servizio della Trasparenza dell'AOUP, per quanto di competenza.

IL DIRETTORE DELL'U.O.C. AFFARI GENERALI
Dott. Vincenzo Manzella

Sul presente atto viene espresso:

parere FAVOREVOLE dal

Il Direttore Sanitario
Dott. Gaetano Cimò

parere FAVOREVOLE dal

Il Direttore Amministrativo
Dott. Sergio Consagra

Il Commissario Straordinario

- Vista la proposta di deliberazione che precede, e che s'intende qui di seguito riportata e trascritta;
- Visto il parere favorevole espresso dal Direttore Amministrativo;
- Visto il parere favorevole espresso dal Direttore Sanitario;
- Ritenuto di condividerne il contenuto;
- Assistito dal segretario verbalizzante;

DELIBERA

Di approvare la superiore proposta, che qui si intende integralmente riportata e trascritta, per come sopra formulata dal Dirigente Responsabile della struttura proponente.

Il Commissario Straordinario
Dott. Maurizio Montalbano

Il segretario verbalizzante
Gabrielle Dourell

AZIENDA OSPEDALIERA UNIVERSITARIA

PUBBLICAZIONE

Si certifica che la presente deliberazione, per gli effetti dell'art. 53 comma 2 L.R. n. 30 del 03/11/1993, in copia conforme all'originale, è stata pubblicata in formato digitale all'albo informatico dell'Azienda Ospedaliera Universitaria Policlinico a decorrere dal giorno 26/11/2023 e che nei 15 giorni successivi:

- ☐ non sono pervenute opposizioni
- ☐ sono pervenute opposizioni da _____

Il Funzionario Responsabile

Gabriella Dorelli

Notificata al Collegio Sindacale il _____

DELIBERA NON SOGGETTA AL CONTROLLO

☒ Delibera non soggetta al controllo, ai sensi dell'art. 4, comma 8 della L. n. 412/1991 e divenuta:

ESECUTIVA

☐ Decorso il termine (10 giorni dalla data di pubblicazione ai sensi dell'art. 53, comma 6, L.R. n. 30/93

☐ Delibera non soggetta al controllo, ai sensi dell'art. 4 comma 8, della L. n. 412/1991 e divenuta:

IMMEDIATAMENTE ESECUTIVA

Ai sensi dell'art. 53, comma 7, L.R. 30/93

Il Funzionario Responsabile

ESTREMI RISCONTRO TUTORIO

☐ Delibera trasmessa, ai sensi della L.R. n. 5/09, all'Assessorato Regionale Salute in data _____ prot. n. _____

SI ATTESTA

Che l'Assessorato Regionale Salute, esaminata la presente deliberazione:

- ☐ Ha pronunciato l'approvazione con atto prot. n. _____ del _____ come da allegato
- ☐ Ha pronunciato l'annullamento con atto prot. n. _____ del _____ come da allegato
- ☐ Delibera divenuta esecutiva con decorrenza del termine previsto dall'art. 16 della L. R. n. 5/09 dal _____

Il Funzionario Responsabile

POLIZIA DI STATO
CENTRO OPERATIVO SICUREZZA
CIBERNETICA POLIZIA POSTALE
E DELLE COMUNICAZIONI
"SICILIA OCCIDENTALE"

AZIENDA OSPEDALIERA UNIVERSITARIA

PROTOCOLLO D'INTESA PER LA PREVENZIONE E CONTRASTO DEI CRIMINI INFORMATICI SUI SISTEMI INFORMATIVI "CRITICI" DIPENDENTI DA AZIENDA OSPEDALIERA UNIVERSITARIA POLICLINICO "P. GIACCONE"

POLIZIA DI STATO
CENTRO OPERATIVO SICUREZZA
CIBERNETICA POLIZIA POSTALE
E DELLE COMUNICAZIONI
"SICILIA OCCIDENTALE"

AZIENDA OSPEDALIERA UNIVERSITARIA

Il Centro Operativo Sicurezza Cibernetica - Polizia Postale e delle Comunicazioni Sicilia Occidentale, con sede in Via Roma 320, rappresentato dal Dirigente, Dott. Marco Scarpa, in qualità di responsabile del coordinamento e controllo delle attività e servizi della Polizia Postale e delle Comunicazioni, nel proprio ambito territoriale,

e

l'Azienda Ospedaliera Universitaria Policlinico "P. Giaccone", con sede in Via Del Vespro n. 129, rappresentata dal Commissario Straordinario, Dott. Maurizio Montalbano,

d'ora innanzi, congiuntamente, le "Parti".

PREMESSO

- che la legge 31 luglio 1997, n. 249, ha istituito l'Autorità per le garanzie nelle comunicazioni dettando norme sui sistemi delle telecomunicazioni e radiotelevisivo;
- che, in relazione all'art. 1, commi 13 e 15 della citata legge, con decreto del Ministro dell'Interno, adottato di concerto con il Ministro delle Comunicazioni e con il Ministro del Tesoro, del Bilancio e della Programmazione Economica, in data 19 gennaio 1999, è stato individuato il Servizio Polizia Postale e delle Comunicazioni del Dipartimento della Pubblica Sicurezza quale organo centrale del Ministero dell'Interno per la sicurezza e la regolarità dei servizi delle telecomunicazioni;
- che l'articolo 39 della legge 16 gennaio 2003, n. 3, recante: *"Disposizioni ordinamentali in materia di pubblica amministrazione"* prevede che il Dipartimento della Pubblica Sicurezza, nell'ambito delle direttive impartite dal Ministro dell'Interno per il potenziamento dell'attività di prevenzione, può stipulare convenzioni con soggetti, pubblici e privati, dirette a fornire, con la contribuzione degli stessi soggetti, servizi specialistici, finalizzati ad incrementare la sicurezza pubblica;
- che il decreto legge 27 luglio 2005 n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005 n. 155, recante "*Misure urgenti per il contrasto del terrorismo internazionale*", ed in Particolare l'art. 7 bis, comma 1, dispone che con decreto del Ministro dell'Interno siano individuate le infrastrutture critiche informatizzate di interesse nazionale, alla cui protezione informatica provvede l'organo del Ministero dell'Interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, operando mediante collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture interessate;
- che il D.P.C.M. del 17 febbraio 2017, recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale, definisce all'art.1 l'architettura istituzionale deputata alla

tutela della sicurezza nazionale relativamente alle infrastrutture critiche materiali e immateriali;

- che il D.P.C.M. del 27 gennaio 2014 ha adottato il "Quadro Strategico Nazionale per la Sicurezza Nazionale dello Spazio Cibernetico" e con DPCM 31/03/2017 è stato ridefinito il "Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica";
- che con il D.Lgs. 18 maggio 2018 n. 51, recante "*Attuazione della Direttiva UE 2016/680 del Parlamento Europeo e del Consiglio del 27 aprile 2016*" sono state ridefinite le regole riguardanti il trattamento dei dati personali effettuato per "finalità di polizia", ovvero direttamente collegate all'attività di prevenzione e repressione dei reati e di tutela dell'ordine e della sicurezza pubblica;
- che con il Decreto 19 settembre 2017, n. 215 del Ministero dell'Interno, di concerto con i Ministri dello Sviluppo Economico e dell'Economia e delle Finanze, è stato adottato il "*Regolamento recante individuazione delle denominazioni, degli stemmi, degli emblemi e degli altri segni distintivi in uso esclusivo alla Polizia di Stato e al Corpo nazionale dei vigili del fuoco, nonché le modalità attuative ai fini della loro concessione in uso temporaneo a terzi*";
- che la Direttiva del Ministro dell'Interno del 15 agosto 2017 "sui comparti delle Specialità e sulla razionalizzazione dei Presidi di Polizia" ha ribadito al punto 1.4 la competenza della Polizia Postale e delle Comunicazioni in materia di protezione delle infrastrutture critiche nonché di sicurezza e regolarità dei servizi di telecomunicazione;
- che nell'ambito della direttiva generale per l'attività amministrativa e per la gestione relativa all'anno 2023, il Ministro dell'Interno, in ordine agli obiettivi operativi, nel ribadire l'esigenza di tutelare dalle minacce cyber coloro che operano nel mondo della rete, anche attraverso appositi contatti bilaterali (intese, riunioni, accordi, ecc.) tra l'amministrazione e gli enti gestori di sistemi e servizi strategici, ha altresì previsto il rafforzamento – attraverso le risorse del PNRR – delle difese cibernetiche, aumentando il grado di resilienza informatica dell'amministrazione attraverso la creazione di sezioni operative per la sicurezza cibernetica distrettuali, di laboratori operativi dotati delle infrastrutture per le attività forensi (CLABS) e il potenziamento della sala server, al fine di prevedere o rilevare tempestivamente attacchi e incidenti informatici;
- che, con decreto del Capo della Polizia Direttore generale della Pubblica Sicurezza, in data 28 giugno 2022, è stata attuata la determinazione dell'assetto ordinativo, dei compiti, delle linee di dipendenza e delle dotazioni organiche delle articolazioni periferiche dell'Amministrazione della Pubblica Sicurezza e, in particolare, dei Centri Operativi per la Sicurezza Cibernetica (C.O.S.C.) quale nuova denominazione dei Compartimenti di Polizia Postale e delle Comunicazioni, al cui interno sono stati istituiti i Nuclei Operativi Sicurezza Cibernetica (N.O.S.C.) adottato ai sensi degli articoli 3 bis, comma 4, e 9 del D.P.R. 22/03/2001 n. 208;

- che con il D.Lgs. 18 maggio 2018 n. 65 è stata recepita la 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*" (c.d. Direttiva NIS), che individua quale Autorità di contrasto il Servizio Polizia Postale e delle Comunicazioni in qualità di organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, di cui all'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n.155, così come individuato dal Decreto Interministeriale del 10 gennaio 1999;
- che il Centro Operativo Sicurezza Cibernetica - Polizia Postale e delle Comunicazioni Sicilia Occidentale provvede, come organo periferico del Servizio Polizia Postale e delle Comunicazioni del Dipartimento della Pubblica Sicurezza, ad assicurare i Servizi della Polizia Postale e delle Comunicazioni, con particolare riferimento alla prevenzione e repressione dei reati commessi avvalendosi delle specifiche potenzialità tecniche dei servizi o mezzi di comunicazione, anche ad alta tecnologia, ovvero alterando il normale funzionamento degli stessi;
- che i sistemi informatici e le reti telematiche di supporto alle funzioni istituzionali dell'Azienda Ospedaliera Universitaria Policlinico "P. Giaccone" sono da considerare infrastrutture sensibili di interesse pubblico. Risulta, pertanto, necessario prevenire e contrastare ogni forma di accesso illecito, anche tentato, con finalità di:
  a) interruzione dei servizi di pubblica utilità;
  b) indebita sottrazione di informazioni;
  c) porre in essere qualsiasi ulteriore attività illecita;
- che a conclusione di specifici incontri tecnici tra i rappresentanti del Centro Operativo Sicurezza Cibernetica e il SIA – Sistema Informatico Aziendale dell'Azienda Ospedaliera Universitaria Policlinico "P. Giaccone" sarà elaborato un modello operativo di collaborazione per la prevenzione ed il contrasto dei crimini informatici che hanno per oggetto, nella loro complessità, i sistemi ed i servizi informatici "critici" dell'Azienda;
- che la cooperazione tra il Centro Operativo Sicurezza Cibernetica - Polizia Postale e delle Comunicazioni Sicilia Occidentale e il SIA – Sistema Informatico Aziendale dell'Azienda Ospedaliera Universitaria Policlinico "P. Giaccone", volta alla prevenzione e alla repressione dei crimini informatici, ispirata al principio di sicurezza partecipata, nell'intento di assicurare in via sinergica ed efficiente le risorse del Sistema Paese a vantaggio dell'intera collettività, contribuisce al contenimento dei costi operativi derivanti da interruzioni dei servizi erogati attraverso sistemi informatici e di telecomunicazioni.

POLIZIA DI STATO
CENTRO OPERATIVO SICUREZZA
CIBERNETICA POLIZIA POSTALE
E DELLE COMUNICAZIONI
"SICILIA OCCIDENTALE"

AZIENDA OSPEDALIERA UNIVERSITARIA

TUTTO CIÒ PREMESSO
LE PARTI STIPULANO E CONVENGONO QUANTO SEGUE

Articolo 1

1. Le Parti si impegnano a sviluppare un piano di collaborazione volto:
   a) alla condivisione e all'analisi di informazioni idonee a prevenire e contrastare attacchi o danneggiamenti in pregiudizio delle infrastrutture informatiche dell'Azienda Ospedaliera Universitaria Policlinico "P. Giaccone" per le finalità meglio in premessa specificate;
   b) alla segnalazione di emergenze relative a vulnerabilità, minacce ed incidenti in danno della regolarità dei servizi di telecomunicazione;
   c) all'identificazione dell'origine degli attacchi che abbiano come destinazione le infrastrutture tecnologiche gestite dall'Azienda Ospedaliera Universitaria Policlinico "P. Giaccone" o che traggano origine dalle medesime;
   d) alla realizzazione e alla gestione di attività di comunicazione fra le Parti per fronteggiare situazioni di emergenza.

2. Le attività necessarie al conseguimento degli obiettivi di cui al precedente comma 1 verranno assicurate dal Centro Operativo Sicurezza Cibernetica e dal SIA – Sistema Informatico Aziendale dell'Azienda Ospedaliera Universitaria Policlinico "P. Giaccone".

Articolo 2

1. Le Parti potranno sviluppare attività formativa congiunta sui sistemi e sulle tecnologie informatiche utilizzate, nonché sulle procedure di intervento atte a prevenire e contrastare gli accessi illeciti o i tentativi di accesso illecito ai danni di tali sistemi e tecnologie nonché i fenomeni delittuosi di cui all'art. 1.

Articolo 3

1. Le Parti cooperano al fine di implementare soluzioni tecnologiche o infrastrutture necessarie per rendere operativo il presente Protocollo d'Intesa, il cui oggetto primario è rappresentato dalla collaborazione da parte della Polizia Postale e delle Comunicazioni, anche attraverso l'interscambio di dati, finalizzata ad incrementare i livelli di prevenzione e contrasto dei crimini informatici ai danni dei sistemi gestiti dall'Azienda Ospedaliera Universitaria Policlinico "P. Giaccone", precisando che gli eventuali oneri, comunque concordati preventivamente, relativi all'attuazione della stessa, sono a carico dell'Azienda Ospedaliera Universitaria Policlinico "P. Giaccone", in coerenza con l'art. 39, comma 2, della L. 16 gennaio 2003, n. 3.

2. Nessun onere economico specifico deriva dal presente accordo per l'Amministrazione della Pubblica Sicurezza.

Articolo 4

1. Le parti si impegnano a sviluppare iniziative congiunte, concordate preventivamente, volte a valorizzare il reciproco rapporto di collaborazione, anche tramite l'utilizzo delle denominazioni, degli stemmi, degli emblemi e degli altri segni distintivi in uso esclusivo alla Polizia di Stato, nel rispetto del decreto del Ministro dell'Interno 19 settembre 2017, n. 215.
2. Con riferimento al precedente comma 1, l'Azienda Ospedaliera Universitaria Policlinico "P. Giaccone" si impegna formalmente a promuovere i rispettivi brand, anche attraverso la realizzazione di spot dedicati da trasmettere su network televisivi e piattaforme social ovvero a mezzo stampa sui principali quotidiani, sempre con il coordinamento del competente Ufficio relazioni esterne, cerimoniale e studi storici della Segreteria del Dipartimento.

Articolo 5

1. Le *Parti* si impegnano a trattare ed a custodire i dati e le informazioni personali acquisite nell'ambito delle attività previste dal presente Protocollo d'Intesa nel rispetto della normativa in materia di protezione dei dati personali.
2. Ciascuna *Parte* si impegna a mantenere riservati ed a non utilizzare i risultati delle attività svolte in comune senza il preventivo consenso scritto dell'altra *Parte*.
3. L'obbligo di riservatezza di cui al comma che precede permarrà anche successivamente all'estinzione del presente Protocollo d'Intesa.

Articolo 6

1. Il presente Protocollo d'Intesa, che entra in vigore dalla data della sottoscrizione, ha durata di tre anni e si rinnoverà tacitamente salvo recesso secondo le modalità di cui al successivo articolo 7.

Articolo 7

1. Ogni controversia relativa all'interpretazione ed all'esecuzione del presente Protocollo d'Intesa viene esaminata bonariamente dalle Parti.
2. Le Parti potranno recedere dal presente accordo senza onere alcuno previo preavviso scritto.

POLIZIA DI STATO
CENTRO OPERATIVO SICUREZZA
CIBERNETICA POLIZIA POSTALE
E DELLE COMUNICAZIONI
"SICILIA OCCIDENTALE"

AZIENDA OSPEDALIERA UNIVERSITARIA

3. A tutti gli effetti di legge, l'Azienda Ospedaliera Universitaria Policlinico "P. Giaccone" dichiara di eleggere domicilio in Palermo, via Del Vespro n. 129.

Letto, approvato e sottoscritto.

Palermo, 21/11/2023

IL DIRIGENTE
DEL CENTRO OPERATIVO PER LA
SICUREZZA CIBERNETICA
POLIZIA POSTALE E DELLE
COMUNICAZIONI
SICILIA OCCIDENTALE
Dott. Marco Scarpa

IL COMMISSARIO STRAORDINARIO
DELL'AOUP "P. GIACCONE"
Dott. Maurizio Montalbano