AZIENDA OSPEDALIERA UNIVERSITARIA

DELIBERAZIONE DELLA DIRETTRICE GENERALE

OGGETTO: Costituzione del Comitato Permanente per la Cybersicurezza (Copecyb) e del Comitato di Crisi per la capacità di risposta aziendale in caso di incidenti.

L'Estensore: Massimo Giuseppe Tartamella

Proposta N. 1658 Del 23/07/2025 Responsabile U.O.C. Sistemi informativi aziendali

Allegati:

Dott. Massimo Giuseppe Tartamella

Firmato da Massimo Giuseppe Tartamella
Data 23-07-2025

Responsabile Unico del Procedimento
Dott. Massimo Giuseppe Tartamella

Firmato da Massimo Giuseppe Tartamella
Data 23-07-2025

Numero imputazione spesa Imputazioni di spesa

Data imputazione spesa

Si autorizza l'imputazione della spesa sul conto e l'esercizio indicati entro il limite del budget annuale assegnato al centro di costo richiedente.

Nulla osta, in quanto conforme alle norme di contabilità.
Il Direttore Area Economica Finanziaria

Parere Assente

Il Direttore Amministrativo

La Direttrice Generale

Dott.ssa Maria Grazia Furnari

Firmato da Maria Grazia Furnari
Data 24-07-2025

Parere Favorevole

Il Direttore Sanitario

Firmato da Alberto Firenze
Data 24-07-2025

La Direttrice Generale dell'AOUP "Paolo Giaccone" di Palermo, Dott.ssa Maria Grazia Furnari, nominata con D.P. n.324 serv.1°/S.G. del 21 giugno 2024 e assistita dal segretario verbalizzante adotta la seguente delibera sulla base della proposta di seguito riportata.

Il Segretario verbalizzante

Firmato da Grazia Scalici
Data 25-07-2025

AZIENDA OSPEDALIERA UNIVERSITARIA

IL RESPONSABILE DELLA UOC SISTEMI INFORMATIVI AZIENDALI

Dott. Massimo Giuseppe Tartamella

PREMESSO CHE

- Il Regolamento Generale sulla Protezione dei Dati (GDPR) - Regolamento UE 2016/679 stabilisce l'obbligo per le aziende sanitarie di proteggere i dati personali dei pazienti e del personale mediante l'adozione di misure tecniche e organizzative adeguate;
- Il D.Lgs. 196/2003, Codice in materia di protezione dei dati personali, modificato dal D.Lgs. 101/2018 che recepisce il GDPR a livello nazionale, specifica ulteriori misure di adeguamento e introduce sanzioni per il mancato rispetto degli obblighi privacy;
- La legge 90/2024 – *Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici* - all'art. 8 stabilisce l'obbligo per tutti i soggetti di cui all'art. 1 comma 1, tra cui rientrano le Aziende Sanitarie, di individuare - nella propria organizzazione aziendale - una struttura responsabile della cybersicurezza al cui interno operi e venga individuato il referente per la cybersicurezza;
- La Direttiva NIS2 -*Network and Information Security* - (Direttiva UE 2022/2555) recepita in Italia con il D.Lgs. 138/2024, ha abrogato la Direttiva NIS1 introducendo requisiti più stringenti per la gestione dei rischi e la risposta agli incidenti, aumentando il numero dei soggetti destinatari degli obblighi di cybersicurezza e obbligando le strutture sanitarie, in quanto rientranti nei "settori ad alta criticità", ad "*adottare misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi per la sicurezza dei sistemi di rete e di informazione che tali soggetti utilizzano per le loro operazioni o per la fornitura dei loro servizi e per prevenire o ridurre al minimo l'impatto degli incidenti sui destinatari dei loro servizi e su altri servizi.*"

VISTA La nota prot. n. 7303 del 03/02/2025 con la quale la Direttrice Generale dell'AOUP ha avviato i lavori propedeutici del "Gruppo di lavoro sulla cybersicurezza";

VISTO Il verbale di seduta del giorno venerdì 27/06/2025, nel quale i membri del "Gruppo di Lavoro sulla cybersicurezza" si costituiscono in "*Comitato permanente*";

CONSIDERATO Che il Comitato permanente avrà il compito, in caso di incidenti, di immediata conoscenza e prima valutazione nonché di porre in essere politiche di sicurezza, in senso ampio, idonee a limitarne la portata e a scongiurare il verificarsi di eventi avversi;

RITENUTO Di dover istituire il Comitato Permanente sulla Cybersicurezza (**Copecyb**); faranno parte del Copecyb, oltre al "punto di contatto NIS2" ovvero del Referente Aziendale per la Cybersicurezza, i seguenti componenti o relativi delegati:

- Responsabile dell'Ufficio Stampa (*Coordinatore*)
- Responsabile dell'U.O.C. Sistemi Informativi Aziendali (*Coordinatore*)
- Responsabile dell'U.O.S. Programmazione e sviluppo aziendale
- Responsabile della Protezione dei Dati Personali (RPD/DPO)
- Coordinatore del Gruppo Aziendale Privacy (G.A.P.)
- Responsabile dell'U.O.S. Formazione
- Servizio di Ingegneria clinica
- Responsabile dell'Area Tecnica

- Responsabile U.O.S. Prevenzione e Protezione
- Rappresentante dell'U.O.C. Risk Management
- Responsabile dell'U.O.S. Comunicazione e URP
- Responsabile U.O.S. Internalizzazione e ricerca sanitaria

Il **Copecyb** si dovrà riunire con cadenza periodica e provvedere alla stesura di un Regolamento interno volto ad indicare le politiche di sicurezza da implementare e da seguire e a scongiurare il verificarsi di eventi che possano compromettere la continuità operativa informatica aziendale.

RITENUTO Di dover, conseguentemente, procedere all'istituzione del Comitato di Crisi così composto:

Presidente: Direttore Generale AOUP;
Coordinatori: Direttore amministrativo e Direttore sanitario;
Vice coordinatori: Responsabile Ufficio Stampa e Responsabile U.O.C. S.I.A.
Componenti: i membri del **Copecyb**;

Che il Comitato di Crisi avrà il compito di:

- porre in essere qualsiasi presupposto decisionale e operativo utile e necessario a garantire la capacità di risposta, in caso di incidente o concreta minaccia di incidente, di qualsiasi natura, al fine di scongiurare il fermo, anche solo temporaneo, delle attività e dei settori strategici dell'Azienda;

TENUTO CONTO

- Informare l'Università degli Studi di Palermo, nei ruoli ritenuti opportuni e necessari;
- Fornire istruzioni rapide e dettagliate, a tutti gli Enti e le professionalità aziendali, idonee a rassicurare circa la solidità e la necessarietà delle scelte intraprese per il mantenimento delle attività lavorative.

TENUTO CONTO Che il **Copecyb** avrà il compito di:
1.Attivarsi nell'immediatezza di una segnalazione di incidente, valutandone la portata, le prevedibili conseguenze, le prime misure da adottare e quelle da realizzare nel prosieguo e/o nel futuro. Riconoscere e adempiere a tutti gli obblighi normativi del caso nonché avviare l'eventuale escalation, verso il Comitato di Crisi, nell'ipotesi di pregiudizio della continuità operativa aziendale con mezzi informatici;
2.Proporre l'adozione di politiche di sicurezza informatica e procedure operative idonee a garantire una protezione efficace, rispetto alle minacce ed alla mitigazione delle conseguenze;
3. Organizzare corsi di formazione e campagne di sensibilizzazione per tutte le Persone che, a vario titolo, operano in Azienda, al fine di promuovere una cultura della sicurezza informatica;
4. Indurre attività di testing ed autovalutazione dell'efficacia delle misure di sicurezza adottate e stimolare le necessarie modifiche, in risposta ad eventuali nuove minacce;
5.Consolidare la prassi operativa volta al controllo ed al coinvolgimento responsabile di tutti i Fornitori esterni, ingaggiati in settori sensibili rispetto alla sicurezza delle infrastrutture, delle reti, dei software e dei servizi on line nonché dei dati personali;

Per i motivi in premessa citati che qui si intendono ripetuti e trascritti

PROPONE DI

istituire il Comitato Permanente per la cybersicurezza (**Copecyb**) come di seguito riportato:

- Responsabile dell'Ufficio Stampa (*Coordinatore*)
- Responsabile dell'U.O.C. Sistemi Informativi Aziendali (*Coordinatore*)
- Responsabile dell'U.O.S. Programmazione e sviluppo aziendale
- Responsabile della Protezione dei Dati Personali (RPD/DPO)
- Coordinatore del Gruppo Aziendale Privacy (G.A.P.)
- Referente Aziendale per la Cybersicurezza (punto di contatto NIS2)
- Responsabile dell'U.O.S. Formazione
- Servizio di Ingegneria clinica
- Responsabile dell'Area Tecnica
- Responsabile U.O.S. Prevenzione e Protezione
- Rappresentante dell'U.O.C. Risk Management
- Responsabile dell'U.O.S. Comunicazione e URP
- Responsabile U.O.S. Internalizzazione e ricerca sanitaria

Con il compito di:

1.Attivarsi nell'immediatezza della segnalazione di un incidente, valutandone la portata, le prevedibili conseguenze, le prime misure da adottare e quelle da realizzare nell'immediato e nel futuro. Riconoscere e adempiere a tutti gli obblighi normativi del caso nonché avviare l'eventuale *escalation,* verso il Comitato di Crisi, nell'ipotesi di pregiudizio della continuità operativa informatica aziendale.

2.Proporre l'adozione di politiche di sicurezza informatica e procedure operative idonee a garantire una protezione efficace, rispetto alle minacce ed alla mitigazione delle conseguenze;

3. Organizzare corsi di formazione e campagne di sensibilizzazione per tutte le Persone che, a vario titolo, operano in Azienda, al fine di promuovere una cultura della sicurezza informatica.

4. Indurre attività di *testing* ed autovalutazione dell'efficacia delle misure di sicurezza adottate e stimolare le necessarie modifiche, in risposta alle nuove minacce.

5.Consolidare una diffusa prassi operativa volta al controllo ed al coinvolgimento responsabile di tutti i Fornitori esterni, ingaggiati in settori sensibili rispetto alla sicurezza delle infrastrutture, delle reti, dei *software* e dei servizi *on line* nonché dei dati personali.

Di dover, conseguentemente, procedere all'istituzione del Comitato di Crisi così composto:

Presidente: Direttore Generale AOUP;
Coordinatori: Direttore amministrativo e Direttore sanitario;
Vice coordinatori: Responsabile Ufficio Stampa e Responsabile U.O.C. S.I.A.

Componenti: i membri del Comitato Permanente per la Cybersicurezza (**Copecyb**).

Con il compito di:

- porre in essere qualsiasi presupposto decisionale e operativo utile e necessario a garantire la capacità di risposta, in caso di incidente o concreta minaccia di incidente, di qualsiasi natura, al fine di scongiurare il fermo, anche solo temporaneo, delle attività e dei settori strategici dell'Azienda;
- Informare l'Università degli Studi di Palermo, nei ruoli ritenuti opportuni e necessari;
- Fornire istruzioni rapide e dettagliate, a tutti gli Enti e le professionalità aziendali, idonee a rassicurare circa la solidità e la necessarietà delle scelte intraprese per il mantenimento delle attività lavorative.

Di dare mandato ai componenti del Comitato Permanente per la Cybersicurezza (Copecyb) di procedere alla stesura di un manuale da diffondere ai dipendenti dell'AOUP.

Di notificare il presente provvedimento al Magnifico Rettore della Università degli studi di Palermo, al Presidente della Scuola di Medicina di Medicina e Chirurgia, ai Direttori dei DAI e a tutto il personale aziendale.

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.