S. Spirito – Fondazione Montel

Azienda Pubblica di Servizi alla Persona

MODELLO ORGANIZZATIVO NIS2

Per la sicurezza e la gestione dei rischi ICT ai sensi della Direttiva (UE) 2022/2025

Percorso organizzativo per la costruzione del documento

Redazione

Data	Nominativo	Ruolo
19/12/2025	BOLGIA CRISTNA	Responsabile Qualità, Innovazione, Formazione e Sicurezza

Verifica

Data	Nominativo	Ruolo
19/12/2025	BERTOLDI GIOVANNI	Direttore Generale

Approvazione

Data	Nominativo	Provvedimento
29/12/2025	CONSIGLIIO DI AMMINISTRAZIONE	Deliberazione n. 89 dd. 29/12/2025

Gruppo di lavoro

Nominativo	Ruolo/qualifica	Servizio/reparto di appartenenza

Data emissione: 29 dicembre 2025

DIFFUSIONE: elenco destinatari

Destinatari	Per competenza e applicazione	Per conoscenza
Direttore Generale		e-mail
Coordinatore Sanitario		e-mail
Economo		e-mail
Responsabile del Personale		e-mail
DPO		e-mail
Amministratore di Sistema		e-mail

Modifiche/revisione al documento

Rev.	Data	Visto per approvazione	Oggetto della modifica

PREMESSA

Il “Modello organizzativo NIS2” rappresenta uno strumento fondamentale per strutturare in modo conforme e funzionale la resilienza digitale dell’azienda. Di seguito viene indicata l’organizzazione definita per la sicurezza informatica, con le figure chiave coinvolte.

OGGETTO E SCOPO

Lo scopo di questo documento è definire in modo chiaro e documentato i ruoli, le responsabilità e le funzioni all’interno dell’organizzazione in materia di cybersecurity e gestione dei rischi informatici, in conformità alla Direttiva UE 2022/2555 (NIS2). In particolare, il documento serve a:

- garantire una governance efficace della sicurezza, individuando chi è responsabile delle politiche operative e tecniche in ambito di sicurezza delle reti e dei sistemi informativi.
- assicurare la conformità agli obblighi normativi, facilitando l’adozione di misure tecniche, organizzative ed operative adeguate, nonché la gestione degli obblighi nei confronti delle autorità competenti.
- favorire la tracciabilità delle azioni, consentendo di ricostruire decisioni, attività e responsabilità in caso di audit o ispezione.

Promuovere una cultura della sicurezza interna, attribuendo chiaramente le responsabilità a tutti i livelli aziendali, dai vertici al personale operativo

CAMPO DI APPLICAZIONE

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 (“NIS2”)

ORGANIGRAMMA

ELENCO DEL PERSONALE COINVOLTO OPERATIVAMENTE NELLA GESTIONE DELLA CYBERSECURITY

COMPARTO	RUOLO	NOMINATIVO/I	DATI DI CONTATTO
Direzione	Responsabile NIS2	Bertoldi Giovanni	Tel: 0461/531002 @: giovanni.bertoldi@apsp-pergine.it
	Punto di Contatto	Bolgia Cristina	Tel. 0461/531002 @ cristina.bolgia@apsp-pergine.it
	Sostituto del Punto di Contatto	Non nominato	
	Referente CSIRT	Puel Diego	@ diego.puel@be-innova.eu
	Sostituto Referente CSIRT	Pilati Ivan	@ ivan.pilati@be-innova.eu
IT	Amministratore di Sistema	Deriu Paolino	@ paolino.deriu@deltainformatica.eu
DPO GDPR	Soggetto referente	Grazioli Matteo	Tel: 0461/390025 @ serviziodpo@upipa.tn.it

REFERENTI NIS2 DI AREA

AREA	RUOLO	NOMINATIVO/I	DATI DI CONTATTO
Economato	Economo	Floriani Selene	Tel. 0461/531002 @ selene.floriani@apsp-pergine.it
Personale	Responsabile del Personale	Bebber Claudia	Tel. 0461/531002 @ claudia.bebber@apsp-pergine.it
Formazione	Responsabile della Formazione	Bolgia Cristina	Tel. 0461/531002 @ cristina.bolgia@apsp-pergine.it

RUOLI CHIAVE E RESPONSABILITÀ

Organo di Amministrazione

- Responsabilità finale per approvare e sovraintendere l'implementazione delle misure di gestione dei rischi di cybersecurity
- Approva politiche di sicurezza
- Garantisce formazione specifica sulla sicurezza informatica
- Verifica periodica del rischio

2. Responsabile NIS2

- Coordinamento generale della compliance

2. Punto di Contatto NIS2

- Interfaccia con ACN
- Gestisce la notifica degli incidenti (24h pre-notifica, 72h notifica dettagliata, 30 giorni relazione finale)

3. Responsabile IT (AdS)

- Adotta le misure tecniche ed organizzative necessarie
- Verifica e gestisce la vulnerabilità e gli accessi
- Verifica e gestisce la sicurezza delle reti, dei sistemi e dei dati

4. CSIRT (Computer Security Incident Response Team)

- Team di risposta agli incidenti di sicurezza informatica
- Monitoraggio continuo e gestione degli incidenti

5. DPO

- Allinea quanto previsto dalla normativa NIS2 con quanto previsto dal GDPR
- Gestisce i data breach
- Effettua le valutazioni d'impatto (DPIA)

6. Referenti NIS2 di area

- Applicano le misure nei processi operativi di riferimento
- Effettuano controlli sui fornitori
- Segnalano eventi anomali


Consiglio di Amministrazione
Detiene la responsabilità finale e strategica sulla sicurezza.
Ruoli Operativi Chiave
Team specializzato per la gestione della sicurezza e degli incidenti.
Responsabile NIS2
Giovanni Bertoldi (Direttore Generale) coordina la compliance
Punto di Contatto
Cristina Bolgia
Interfaccia con le autorità competenti (ACN)
Responsabile IT
Paolino Deriu
Gestione tecnica della sicurezza di sistemi e reti
Referente CSIRT
Diego Puel
Team di risposta agli incidenti di sicurezza
DPO/RDP
Matte Grazioli
Allineamento con la normativa GDPR
Responsabilità Chiave per la Sicurezza
Organo di Amministrazione: Supervisione Strategica
Approva le politiche di sicurezza e garantisce la formazione sui rischi informatici.
Punto di Contatto: Gestione Notifiche Incidenti
Comunica gli incidenti alle autorità: pre-notifica (24h), notifica (72h), relazione finale (30gg).
CSIRT & Resp. IT: Difesa Tecnica e Risposta
Monitorano, gestiscono vulnerabilità e rispondono attivamente agli incidenti.
Referenti di Area: Applicazione e Controllo Quotidiano
Applicano le misure nei processi operativi e segnalano eventi anomali.
NotebookLM