PSI POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

Rev.0 13.05.2024

Dichiarazione generale di politica per la sicurezza

1. SCOPO E CAMPO DI APPLICAZIONE DEL DOCUMENTO

Lo scopo del presente documento è quello di descrivere i principi generali di sicurezza delle informazioni definiti dall' **U.O.C. Sistemi Informativi** al fine di sviluppare un efficiente e sicuro Sistema di Gestione della Sicurezza delle Informazioni.

2. RIFERIMENTI

- ISO/IEC 27001:2022 Information technology – Security techniques - Information security management systems – Requirements
- Decreto legislativo 30 giugno 2003, n. 196 – Provvedimenti del Garante
- Nuovo Regolamento Europeo DGPR 679/2016 in materia di protezione dei dati personali

3. RESPONSABILITÀ ED AGGIORNAMENTI

La politica della sicurezza delle informazioni viene costantemente aggiornata per assicurare il suo continuo miglioramento ed è condivisa con l'organizzazione, le terze parti ed i clienti, attraverso un sistema documentale interno e specifici canali di comunicazione.

La **U.O.C. Sistemi Informativi** dell'AORN S.G. Moscati è responsabile del sistema di gestione sicura delle informazioni, in coerenza con l'evoluzione del contesto aziendale, valutando eventuali azioni da intraprendere a fronte di eventi come:

- evoluzioni significative del business;
- nuove minacce rispetto a quelle considerate nell'attività di analisi del rischio;
- significativi incidenti di sicurezza;
- evoluzione del contesto normativo o legislativo in materia di trattamento sicuro delle informazioni;

4. SCOPO DELL'ORGANIZZAZIONE

L'**U.O.C. Sistemi Informativi** ha come missione strategica la gestione ed erogazione di servizi informatici con relativi servizi di assistenza e manutenzione nell'ambito Ospedaliero.

Il sistema di gestione, nella sua formulazione e attuazione, risponde a tutti i requisiti normativi che vanno dal 4 al 10.
Non ci sono esclusioni e quindi la stessa organizzazione dichiara la conformità del proprio sistema alla Norma internazionale. **La nostra organizzazione applica tutti i controlli di sicurezza previsti dall'appendice A della Norma ISO 27001:2022.**

5. FINALITÀ STRATEGICA

Per l'**U.O.C. Sistemi Informativi** la sicurezza delle informazioni ha come obiettivo primario la protezione dei dati e delle informazioni, della struttura tecnologica, fisica, logica ed organizzativa, e la loro gestione. Questo significa ottenere e mantenere un sistema di gestione sicura delle informazioni, attraverso il rispetto delle seguenti proprietà:

1. **Riservatezza:** assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati;
2. **Integrità:** salvaguardare la consistenza dell'informazione da modifiche non autorizzate;
3. **Disponibilità:** assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali associati quando ne fanno richiesta;

la Politica è accessibile sul sito internet dell'organizzazione

4. **Controllo:** assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati;
5. **Autenticità:** garantire una provenienza affidabile dell'informazione.
6. **Privacy:** garantire la protezione ed il controllo dei dati personali.

Consapevoli che i dati dell'utente, i risultati della loro analisi, gli indirizzi suggeriti e i metodi di indagine costituiscono informazioni il cui valore rappresenta il patrimonio dell'organizzazione e di quella dell'utente, abbiamo implementato un sistema di gestione per la sicurezza delle informazioni seguendo i requisiti specificati della Norma ISO 27001:2022 e delle leggi cogenti come mezzo per gestire la sicurezza delle informazioni e prevedendo la messa a punto di tutti i controlli di sicurezza applicabili al trattamento delle informazioni.

6. AMBITO DI APPLICAZIONE

La politica per la sicurezza delle informazioni dell'**U.O.C. Sistemi Informativi** si applica a tutto il personale interno ed alle terze parti che collaborano alla gestione delle informazioni ed a tutti i processi e risorse coinvolte nell'erogazione di servizi informatici con relativi servizi di assistenza e manutenzione nell'ambito Ospedaliero.

7. POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

La politica della sicurezza dell'**U.O.C. Sistemi Informativi** rappresenta l'impegno dell'organizzazione nei confronti degli utenti e terze parti a garantire la sicurezza delle informazioni, degli strumenti fisici, logici e organizzativi atti al trattamento delle informazioni in tutte le attività.

La politica della sicurezza delle informazioni dell'U.O.C. Sistemi Informativi si ispira ai seguenti principi:

1. Garantire all'organizzazione la piena conoscenza delle informazioni gestite e la valutazione della loro criticità, al fine di agevolare l'implementazione degli adeguati livelli di protezione.
2. Garantire l'accesso sicuro alle informazioni, in modo da prevenire trattamenti non autorizzati o realizzati senza i diritti necessari.
3. Garantire che l'organizzazione e le terze parti collaborino al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza.
4. Garantire che le anomalie e gli incidenti aventi ripercussioni sul sistema informativo e sui livelli di sicurezza aziendale siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business.
5. Garantire che l'accesso alle sedi ed ai singoli locali aziendali avvenga esclusivamente da personale autorizzato, a garanzia della sicurezza delle aree e degli asset presenti.
6. Garantire la conformità con i requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con le terze parti.
7. Garantire la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi al fine di rispettare la sicurezza e la disponibilità dei servizi e delle informazioni.
8. Garantire la business continuity aziendale e il disaster recovery, attraverso l'applicazione di procedure di sicurezza stabilite.
9. Garantire risorse adeguate, aggiornate e adeguatamente qualificate per la sicurezza delle informazioni

la Politica è accessibile sul sito internet dell'organizzazione

PSI POLITICA PER LA SICUREZZA DELLE INFORMAZIONI Rev.0 13.05.2024

La politica della sicurezza delle informazioni dell'U.O.C. Sistemi Informativi persegue i seguenti obiettivi:

1) **rispettare** le leggi e le disposizioni vigenti, i requisiti contrattuali e le procedure in essere, conformandosi ai principi e ai controlli stabiliti dalla ISO/IEC 27001:2022 o altre norme/regolamenti che disciplinano le attività in cui opera, tra i quali, in particolare le regolamentazioni inerenti ai trattamenti dei dati personali e la loro sicurezza.

2) **dimostrare** agli stakeholders la propria capacità di fornire con regolarità la gestione ed erogazione di servizi informatici con relativi servizi di assistenza e manutenzione nell'ambito Ospedaliero, massimizzando gli obiettivi di sicurezza, anche promuovendo la collaborazione, comprensione e consapevolezza da parte dei fornitori strategici;

3) **minimizzare** il rischio di perdita e/o indisponibilità dei dati gestiti, pianificando e gestendo le attività a garanzia della continuità di servizio, svolgendo una continua ed adeguata analisi dei rischi che esamini costantemente le vulnerabilità e le minacce associate alle attività a cui si applica il sistema, controllando con continuità il corretto funzionamento degli asset aziendali al fine di rilevare eventi anomali, incidenti e vulnerabilità dei sistemi informativi per rispettare la sicurezza e la disponibilità dei servizi e delle informazioni;

4) **migliorare** con continuità il sistema di sicurezza delle informazioni al fine di rendere sempre più efficiente e sicuro il sistema informativo.

Politica per l'impegno per il miglioramento continuo del sistema di gestione

Il patrimonio informativo dell'utente e quello relativo al know-how dell'organizzazione costituiranno d'ora innanzi i punti focali dell'impegno di tutti. Un impegno assunto da tutti e da ciascuno.

Tale impegno sarà manifestato attraverso le "performance di sicurezza" che dovranno dare evidenza di quanto la nostra organizzazione ed il nostro sistema di gestione della sicurezza delle informazioni siano efficaci nel registrare un miglioramento continuo.

Predisposizione	Approvazione
RSGSI:	**DIR:**

la Politica è accessibile sul sito internet dell'organizzazione