Allegato 1

Il presente documento integra l'Accordo e ne costituisce parte integrante, al fine di indicare il servizio erogato e, conseguentemente, di specificare le condizioni alle quali il Centro Servizi effettua trattamenti di dati personali per conto dell'Azienda.

Servizio	**Accesso ai sistemi CUP / CUP WEB (piattaforme dell'Azienda ULSS) per la prenotazione di prestazioni erogabili agli utenti, e conseguente scarico dei referti**
Ruolo dell'Azienda	Titolare del trattamento
Ruolo del Centro Servizi	Responsabile del trattamento
Categorie di interessati	✔ ospiti/utenti del Centro Servizi; ✔ dipendenti/collaboratori a cui sono assegnate utenze informatiche.
Categorie di dati	✔ dati personali di natura comune (es. dati anagrafici degli ospiti; dati anagrafici e account degli utenti); ✔ dati personali di natura particolare ex art. 9 GDPR (es. dati relativi alla salute, in relazione a quanto strettamente necessario per l'erogazione della prestazione).
Finalità del trattamento	✔ esecuzione della prenotazione delle prestazioni e scarico dei referti
Attività che il Centro Servizi potrà svolgere	✔ registrazione; ✔ organizzazione e strutturazione; ✔ conservazione e protezione; ✔ accesso e consultazione; ✔ adattamento e modifica dei dati; ✔ estrazione; ✔ comunicazione mediante trasmissione; ✔ cancellazione e distruzione.
Altri trattamenti	Ogni altro trattamento previsto dalla convenzione.
Durata del trattamento	Fino all'esecuzione della prestazione e, comunque, fino alla cessazione del Rapporto
Trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale	Non previsto
Ulteriori Responsabili / Sub Responsabili	*** da specificare, nel caso in cui vi sia l'utilizzo del servizio da parte di ulteriori soggetti (es. cooperativa di servizi) ***
Disciplina della cessazione del Contratto	Alla cessazione del Contratto, il Centro Servizi mette a disposizione dell'Azienda i dati per il ritiro, dandogliene comunicazione per iscritto e provvedendo alla cancellazione definitiva dei dati dai propri sistemi - astenendosi da ogni ulteriore trattamento salvo che la legge preveda la conservazione dei dati per specifici motivi - qualora l'Azienda non dia indicazioni diverse con comunicazione scritta entro i successivi 90 giorni.

Allegato 2

Il presente documento integra l'Accordo e ne costituisce parte integrante, al fine di indicare il servizio erogato e, conseguentemente, di specificare le rispettive responsabilità.

Servizio	**Assistenza medica**
Ruolo dell'Azienda	Titolare autonomo del trattamento
Ruolo del Centro Servizi	Titolare autonomo del trattamento
Ripartizione dei ruoli	L'attività di assistenza medica a favore degli ospiti non autosufficienti presenti presso il Centro Servizi o comunque svolte presso il Centro Servizi da personale medico dell'Azienda è eseguita dall'Azienda stessa con tale ruolo di titolare autonomo. Per ogni ulteriore attività di trattamento che riguardi i dati personali degli ospiti, che derivi da quanto sopra e che sia svolta dal Centro Servizi, la titolarità spetta a quest'ultimo. Nell'ambito del servizio in oggetto l'Azienda e il Centro Servizi perseguono pertanto distinte finalità, definendo queste, e i mezzi del trattamento, in autonomia; pertanto, la comunicazione dei dati personali relativi all'interessato avviene tra titolari autonomi.

Allegato 3

Il presente documento integra l'Accordo e ne costituisce parte integrante, al fine di indicare il servizio erogato e, conseguentemente, di specificare le rispettive responsabilità.

Servizio	**Assistenza medico specialistica**
Ruolo dell'Azienda	Titolare del trattamento
Ruolo del Centro Servizi	Titolare del trattamento
Ripartizione dei ruoli	L'attività di assistenza medico specialistica è svolta dall'Azienda mediante strutture e personale interni o convenzionati e/o accreditati, con tale ruolo di titolare autonomo. Per ogni ulteriore attività di trattamento che riguardi i dati personali degli ospiti, che derivi da quanto sopra e che sia svolta dal Centro Servizi, la titolarità spetta a quest'ultimo. Nell'ambito del servizio in oggetto l'Azienda e il Centro Servizi perseguono pertanto distinte finalità, definendo queste, e i mezzi del trattamento, in autonomia; pertanto, la comunicazione dei dati personali relativi all'interessato avviene tra titolari autonomi.

Allegato 4

Il presente documento integra l'Accordo e ne costituisce parte integrante, al fine di indicare il servizio erogato e, conseguentemente, di specificare le rispettive responsabilità.

Servizio	**Attività di riabilitazione**
Ruolo dell'Azienda	Titolare del trattamento
Ruolo del Centro Servizi	Titolare del trattamento
Ripartizione dei ruoli	L'attività di riabilitazione è svolta dall'Azienda mediante strutture e personale interni o convenzionati e/o accreditati, con tale ruolo di titolare autonomo. Per ogni ulteriore attività di trattamento che riguardi i dati personali degli ospiti, che derivi da quanto sopra e che sia svolta dal Centro Servizi, la titolarità spetta a quest'ultimo. Nell'ambito del servizio in oggetto l'Azienda e il Centro Servizi perseguono pertanto distinte finalità, definendo queste, e i mezzi del trattamento, in autonomia; pertanto, la comunicazione dei dati personali relativi all'interessato avviene tra titolari autonomi.

Allegato 5

Il presente documento integra l'Accordo e ne costituisce parte integrante, al fine di indicare il servizio erogato e, conseguentemente, di specificare le rispettive responsabilità.

Servizio	**Erogazione di protesi e ausili**
Ruolo dell'Azienda	Titolare del trattamento
Ruolo del Centro Servizi	Titolare del trattamento
Ripartizione dei ruoli	L'erogazione di protesi e ausili è svolta dall'Azienda sulla base di protocolli di intesa tra medico curante e medico coordinatore dell'Azienda, tramite strutture e personale interni o convenzionati e/o accreditati all'Azienda medesima, con tale ruolo di titolare autonomo. Per ogni ulteriore attività di trattamento che riguardi i dati personali degli ospiti, che derivi da quanto sopra e che sia svolta dal Centro Servizi, la titolarità spetta a quest'ultimo. Nell'ambito del servizio in oggetto l'Azienda e il Centro Servizi perseguono pertanto distinte finalità, definendo queste, e i mezzi del trattamento, in autonomia; pertanto, la comunicazione dei dati personali relativi all'interessato avviene tra titolari autonomi.

Allegato 6

Il presente documento integra l'Accordo e ne costituisce parte integrante, al fine di indicare il servizio erogato e, conseguentemente, di specificare le rispettive responsabilità.

Servizio	**Fornitura di farmaci**
Ruolo dell'Azienda	Titolare del trattamento
Ruolo del Centro Servizi	Titolare del trattamento
Ripartizione dei ruoli	La fornitura di farmaci è svolta dall'Azienda, tramite strutture e personale interni o esterni, con tale ruolo di titolare autonomo. Per ogni ulteriore attività di trattamento che riguardi i dati personali degli ospiti, che derivi da quanto sopra e che sia svolta dal Centro Servizi, la titolarità spetta a quest'ultimo. Nell'ambito del servizio in oggetto l'Azienda e il Centro Servizi perseguono pertanto distinte finalità, definendo queste, e i mezzi del trattamento, in autonomia; pertanto, la comunicazione dei dati personali relativi all'interessato avviene tra titolari autonomi.

Allegato 7

Il presente documento integra l'Accordo e ne costituisce parte integrante, al fine di indicare il servizio erogato e, conseguentemente, di specificare le rispettive responsabilità.

Servizio	**Fornitura di alimentazione artificiale**
Ruolo dell'Azienda	Titolare del trattamento
Ruolo del Centro Servizi	Titolare del trattamento
Ripartizione dei ruoli	La fornitura di alimentazione artificiale è svolta dall'Azienda, tramite strutture e personale interni, con tale ruolo di titolare autonomo. Per ogni ulteriore attività di trattamento che riguardi i dati personali degli ospiti, che derivi da quanto sopra e che sia svolta dal Centro Servizi, la titolarità spetta a quest'ultimo. Nell'ambito del servizio in oggetto l'Azienda e il Centro Servizi perseguono pertanto distinte finalità, definendo queste, e i mezzi del trattamento, in autonomia; pertanto, la comunicazione dei dati personali relativi all'interessato avviene tra titolari autonomi.

Allegato 8

Il presente documento integra l'Accordo e ne costituisce parte integrante, al fine di indicare il servizio erogato e, conseguentemente, di specificare le rispettive responsabilità.

Servizio	**Erogazione di presidi**
Ruolo dell'Azienda	Titolare del trattamento
Ruolo del Centro Servizi	Titolare del trattamento
Ripartizione dei ruoli	L'erogazione di presidi è svolta dall'Azienda, tramite strutture e personale interni o convenzionati e/o accreditati all'Azienda medesima, con tale ruolo di titolare autonomo. Per ogni ulteriore attività di trattamento che riguardi i dati personali degli ospiti, che derivi da quanto sopra e che sia svolta dal Centro Servizi, la titolarità spetta a quest'ultimo. Nell'ambito del servizio in oggetto l'Azienda e il Centro Servizi perseguono pertanto distinte finalità, definendo queste, e i mezzi del trattamento, in autonomia; pertanto, la comunicazione dei dati personali relativi all'interessato avviene tra titolari autonomi.

Allegato 9

Il presente documento integra l'Accordo e ne costituisce parte integrante, al fine di indicare il servizio erogato e, conseguentemente, di specificare le rispettive responsabilità.

Servizio	**Condivisione documentazione e informazioni conseguenti ad incontri U.V.M.D.**
Ruolo dell'Azienda	Titolare del trattamento
Ruolo del Centro Servizi	Titolare del trattamento
Ripartizione dei ruoli	Al fine di completare il fascicolo dell'ospite già assegnato da graduatoria regionale al Centro servizi, e consentirne pertanto l'ammissione ai trattamenti di residenzialità secondo le specifiche caratteristiche di quest'ultimo, si rende necessario poter procedere con la condivisione della documentazione derivante da incontri di U.V.M.D. (quali ad esempio la scheda SVAMA). Nell'ambito di tale attività l'Azienda e il Centro Servizi perseguono pertanto distinte finalità, definendo queste, e i mezzi del trattamento, in autonomia; pertanto, la comunicazione dei dati personali relativi all'interessato avviene tra titolari autonomi, e percorre esclusivamente il fine di alleggerire di ulteriori oneri l'ospite stesso o i suoi familiari.

Oggetto: Adeguamento Regolamento Generale sulla Protezione dei Dati - UE 2016/679

A seguito dell'applicazione del Regolamento generale per la protezione dei dati personali *(di seguito GDPR),* entrato in vigore il 25 maggio 2016 ed efficace dal 25 maggio, si porta alla Vostra attenzione quanto specificato nel testo del Regolamento, ed in particolare agli artt. 25, 32, 33, 34 e 35, recanti indicazioni in merito alla sicurezza dei dati personali.

Differentemente da quanto è previsto con il previgente Codice D.lgs. 196/2003, che individuava alcune misure minime di sicurezza, dettagliate nell'allegato B, il GDPR introduce il concetto di "*...misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio...*", andando a definire un elenco non esaustivo di quanto dovrebbe essere applicato ad ogni singola attività di trattamento.

Il GDPR introduce il principio di *accountability (tradotto in "responsabilizzazione")*, ovvero la capacità di dimostrare di aver applicato ogni misura si ritenga utile e necessaria, al fine di garantire la sicurezza nelle attività di trattamento.

In quest'ottica quindi, non ci si limita più a valutare un livello "minimo" di sicurezza, ma si introducono vari elementi che impongono una valutazione sulle misure idonee a garantire un'adeguata sicurezza nelle attività di trattamento, tra le altre, se del caso:

- **Protezione dei dati fin dalla progettazione**: In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i fornitori dei prodotti, dei servizi e delle applicazioni dovrebbero tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati;
- **Protezione per impostazione predefinita:** garantire che l'attività di trattamento, per impostazione predefinita, avvenga solamente relativamente a dati personali necessari per ogni singola specifica finalità;
- **Pseudonimizzazione**: trattamento dei dati personali in modo tale che gli stessi non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che queste siano conservate separatamente e soggette a misure tecniche e organizzative tali da ridurre al minimo i rischi di conoscenza accidentale e di accesso abusivo o non autorizzato;
- **Cifratura** dei dati personali, ovvero rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi;
- **Capacità** di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- **Capacità di ripristinare** tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- **Procedure per testare**, verificare e valutare regolarmente **l'efficacia** delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
- Adesione a un **codice di condotta** di cui all'articolo 40 del GDRP;
- **Certificazione** nonché rilascio di sigilli e marchi di protezione dei dati, secondo quando disposto all'articolo 42 del GDPR;
- **Sistemi di controllo** per evitare o arginare casi di violazione dei dati personali (data breach);
- **Valutazione d'impatto sulla protezione dei dati**, secondo quanto previsto dall'art. 35 del GDPR, realizzata direttamente dal fornitore sul prodotto/servizio che va ad offrire;
- **Ogni ulteriore elemento ritenuto utile** dal fornitore per garantire un livello di sicurezza adeguato al rischio.

- **Sistemi di controllo** per evitare o arginare casi di violazione dei dati personali (data breach);
- **Valutazione d'impatto sulla protezione dei dati**, secondo quanto previsto dall'art. 35 del GDPR, realizzata direttamente dal fornitore sul prodotto/servizio che va ad offrire;
- **Ogni ulteriore elemento ritenuto utile** dal fornitore per garantire un livello di sicurezza adeguato al rischio.

Il GDPR dispone inoltre che il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale sia ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantisce un livello di protezione adeguato.

A tal motivo, dovranno anche essere fornite informazioni in merito ad eventuale trasferimento / trattamento dei dati con i Vs prodotti e/o servizi in paesi extra territorio UE, specificando i soggetti terzi coinvolti, i territori nei quali queste risiedono, ovvero dove sono dislocati i dati, e le garanzie applicate: si ricorda ad esempio che ricadono in questa analisi sistemi di storage in Cloud su server dislocati in territorio extra UE, oppure accesso da parte di altre società (*partecipate o controllate, partner, etc....)* ai prodotti / servizi da Voi offerti.

Relativamente ai servizi affidati in ***Cloud*** - IaaS, SaaS, PaaS- si devono poi proporre maggiori informazioni, sia sul fornitore che sul servizio stesso, con particolare riguardo a:

- Affidabilità del fornitore *(esperienza, capacità e affidabilità del fornitore; caratteristiche della connettività; qualificazione del personale impiegato)*;
- Portabilità dei dati *(sono ovviamente privilegiati i servizi che lo favoriscono)*;
- Garanzie sulla disponibilità e sulle prestazioni dei servizi in cloud *(garanzie sulla riservatezza e sulla continuità operativa)*;
- Dislocazione dei server ed eventuali dipendenze da altri fornitori;
- Tempi e modalità di archiviazione e conservazione dei dati;
- Tutele legali *(responsabilità, compliance, legge applicabile, foro competente).*

Sul punto si richiamano le seguenti fonti:

- Gruppo di Lavoro art. 29 (WP29): Parere 05/2012 sul *cloud computing*, adottato il primo luglio 2012;
- Garante per la protezione dei dati personali: *Cloud computing* – La guida del Garante della Privacy per imprese e pubblica amministrazione (24 maggio 2012);
- Banca d'Italia: Circolare n. 263 del 27 dicembre 2006, 15° aggiornamento del 2 luglio 2015;
- European Banking Authority: Recommendations on outsourcing to cloud service providers (EBA/REC/2017/03, 20 dicembre 2017);
- Ulteriori numerosi documenti a cura dell'ENISA, della CONSIP e dell'AGID emanati nel tempo.

Si chiede, pertanto, di compilare e di produrre – su eventuale richiesta della scrivente - specifica documentazione attestante l'adeguatezza dei prodotti/servizi proposti alla scrivente, con particolare attenzione a quanto esplicitato.

Qualora il fornitore non abbia già propria documentazione attestante quanto richiesto, si riporta di seguito un esempio di schema di misure di sicurezza redatto secondo metodologia ENISA.

REGIONE DEL VENETO
ULSS 1 DOLOMITI

Oggetto: Adeguamento Regolamento Generale sulla Protezione dei Dati - UE 2016/679

A seguito dell'applicazione del Regolamento generale per la protezione dei dati personali *(di seguito GDPR),* entrato in vigore il 25 maggio 2016 ed efficace dal 25 maggio, si porta alla Vostra attenzione quanto specificato nel testo del Regolamento, ed in particolare agli artt. 25, 32, 33, 34 e 35, recanti indicazioni in merito alla sicurezza dei dati personali.

Differentemente da quanto è previsto con il previgente Codice D.lgs. 196/2003, che individuava alcune misure minime di sicurezza, dettagliate nell'allegato B, il GDPR introduce il concetto di "*...misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio...*", andando a definire un elenco non esaustivo di quanto dovrebbe essere applicato ad ogni singola attività di trattamento.

Il GDPR introduce il principio di *accountability (tradotto in "responsabilizzazione")*, ovvero la capacità di dimostrare di aver applicato ogni misura si ritenga utile e necessaria, al fine di garantire la sicurezza nelle attività di trattamento.

In quest'ottica quindi, non ci si limita più a valutare un livello "minimo" di sicurezza, ma si introducono vari elementi che impongono una valutazione sulle misure idonee a garantire un'adeguata sicurezza nelle attività di trattamento, tra le altre, se del caso:

- **Protezione dei dati fin dalla progettazione**: In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i fornitori dei prodotti, dei servizi e delle applicazioni dovrebbero tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati;
- **Protezione per impostazione predefinita:** garantire che l'attività di trattamento, per impostazione predefinita, avvenga solamente relativamente a dati personali necessari per ogni singola specifica finalità;
- **Pseudonimizzazione**: trattamento dei dati personali in modo tale che gli stessi non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che queste siano conservate separatamente e soggette a misure tecniche e organizzative tali da ridurre al minimo i rischi di conoscenza accidentale e di accesso abusivo o non autorizzato;
- **Cifratura** dei dati personali, ovvero rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi;
- **Capacità** di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- **Capacità di ripristinare** tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- **Procedure per testare**, verificare e valutare regolarmente **l'efficacia** delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
- Adesione a un **codice di condotta** di cui all'articolo 40 del GDRP;
- **Certificazione** nonché rilascio di sigilli e marchi di protezione dei dati, secondo quando disposto all'articolo 42 del GDPR;

Il sottoscritto ARRIGO BOITO, nato il 16/7/72, a BELLUNO

Legale rappresentante della Ditta Servizi Alla Persona Longarone Zoldo a.s.c.

con la qualifica di (titolare, socio, procuratore, ecc.) DF C.F. BTORRG72L16A757L

SEDE LEGALE in LONGARONE via BARZAN 6

PARTITA IVA 01187850258 **CODICE FISCALE** _____

Visto ed esaminato quanto sopra indicato, conformemente a quanto previsto dal Regolamento Generale sulla protezione dei dati - UE 2016/679,

dichiara

che la Ditta Servizi alla Persona Longarone Zoldo a.s.c. ha adottato idonee misure atte a garantire un'adeguata sicurezza nelle attività di trattamento dei dati.
A tal fine produce la seguente documentazione attestante l'adeguatezza dei prodotti/servizi proposti:

1) *Schema di misure di sicurezza, redatto secondo metodologia ENISA.*
2) *Riportare l'eventuale ulteriore documentazione presentata..*
3) ..

Data 28/12/24

SERVIZI ALLA PERSONA Longarone Zoldo a.s.c.
Via B. Lorgna, 6 - 32013 Longarone (BL)
Tel.0437-770392 C.F. / P.IVA 01187850258

firma digitale del firmatario

MISURE TECNICHE ED ORGANIZZATIVE SECONDO LA METODOLOGIA ENISA

CATEGORIA DI APPARTENENZA DELLA MISURA DI SICUREZZA	PRESENTE (SI/NO) *Ove applicabile, motivare la scelta, dettagliando quanto possibile*
Politica di sicurezza e procedure per la protezione dei dati personali	
Viene documentata la propria politica in merito al trattamento dei dati personali come parte della sua politica di sicurezza delle informazioni.	SI
Ruoli e responsabilità	
I ruoli e le responsabilità relativi al trattamento dei dati personali sono chiaramente definiti e assegnati in conformità con le politiche di sicurezza.	SI
Per le attività che il fornitore, in qualità di responsabile del trattamento dei dati personali, effettua per conto del Titolare con il supporto di ulteriori sub fornitori, gli obblighi in materia di protezione dei dati sono imposti parimenti a questi - mediante contratto o altro atto giuridico – e l'elenco di tali soggetti è comunicata al Titolare, ed aggiornato ad ogni variazione.	SI
Politica di controllo degli accessi	
I diritti specifici di controllo degli accessi sono assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio della stretta pertinenza e necessità per il ruolo di accedere e conoscere i dati.	In Azienda Speciale Limana Servizi è presente un dominio active directory windows server 2019 dove ogni utente è diviso per gruppi (infermieri/amministrazione/...) e ogni gruppo ha accesso alle risorse ad esso destinate, i programma zucchetti/cba ha un sistema di accesso diviso per utenti (integrati nel programma)
Gestione risorse/asset	
L'organizzazione dispone di un registro/censimento delle risorse e degli apparati IT utilizzati per il trattamento dei dati personali (hardware, software e rete). Il registro include almeno le seguenti informazioni: risorsa IT, tipo (ad es. Server, workstation), posizione (fisica o elettronica). È stato assegnato ad una persona specifica il compito di mantenere e aggiornare il registro (ad esempio, il responsabile IT).	Non è presente

CATEGORIA DI APPARTENENZA DELLA MISURA DI SICUREZZA	PRESENTE (SI/NO) *Ove applicabile, motivare la scelta, dettagliando quanto possibile*
Gestione delle modifiche apportate alle risorse, agli apparati ed ai sistemi IT	
L'organizzazione si assicura che tutte le modifiche alle risorse, agli apparati ed al sistema IT sono registrate e monitorate da una persona specifica (ad esempio, il Responsabile IT o sicurezza). Il monitoraggio regolare delle eventuali delle modifiche apportate al sistema IT avviene con cadenza almeno annuale.	Si
Lo sviluppo software viene eseguito in un ambiente speciale non collegato al sistema IT utilizzato per il trattamento dei dati personali. Se eseguito un test, vengono utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non è possibile, sono previste procedure specifiche per la protezione dei dati personali utilizzati nei test e nello sviluppo software.	--
Sono previste e applicate alcune policy interne che disciplinano la gestione delle modifiche e che includono per lo meno: un processo che governa l'introduzione delle modifiche, i ruoli / utenti che hanno i diritti di modifica, le tempistiche per l'introduzione delle modifiche. La policy di gestione delle modifiche è regolata con cadenza almeno annuale.	--
Gestione degli incidenti / Violazione dei dati personali (*Personal data breaches*)	
È stato definito un piano di risposta agli incidenti (*Incident Response Plan*) con procedure dettagliate per garantire una risposta efficace e ordinata al verificarsi di incidenti o violazioni di dati personali.	Si è stato predisposto, anche se non è ancora attivo, un foglio con le procedure previste in caso di incidente hw/sw
Obblighi di confidenzialità imposti al personale	
L'organizzazione garantisce che tutti i dipendenti, lavoratori e persone autorizzate al trattamento comprendano le proprie responsabilità e gli obblighi di riservatezza sui dati personali oggetto del trattamento da essi svolto. I ruoli e le responsabilità devono essere chiaramente definiti ed assegnati comunicati durante il processo di preassunzione e / o assunzione.	Si
Formazione	
L'organizzazione garantisce che tutti i dipendenti, lavoratori e persone autorizzate al trattamento siano adeguatamente formati e informati sui controlli di sicurezza del sistema informatico relativi al loro lavoro quotidiano. I dipendenti coinvolti nel trattamento dei dati personali devono inoltre essere adeguatamente informati in merito ai requisiti e agli obblighi legali in materia di protezione dei dati attraverso	Sono in programma dei corsi di formazione che inizieranno nel mese di novembre 2024

CATEGORIA DI APPARTENENZA DELLA MISURA DI SICUREZZA	PRESENTE (SI/NO) *Ove applicabile, motivare la scelta, dettagliando quanto possibile*
regolari campagne di sensibilizzazione o iniziative di formazione specifica.	
Generazione di file di log e monitoraggio	
Vengono registrate le azioni degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta / cancellazione / modifica dei diritti dell'utente.	È in fase di implementazione in (wazuh) un sistema che raccoglie i logs dei server e del firewall e NAS
Backup	
Le copie dei backup vengono crittografate e archiviate in modo sicuro, anche offline.	Sì (Acronis con pwd x criptazione dei backups)
Sicurezza del ciclo di vita delle applicazioni	
Durante lo sviluppo del ciclo di vita vengono seguite le migliori pratiche, lo stato dell'arte e pratiche di sviluppo, framework o standard di protezione sicuri ben noti.	--
Specifici requisiti di sicurezza vengono definiti durante le prime fasi del ciclo di vita dello sviluppo.	--
Le tecnologie e le tecniche specifiche progettate per supportare la privacy e la protezione dei dati (denominate anche tecnologie di miglioramento della privacy (PET) vengono adottate in analogia con i requisiti di sicurezza. Vanno valutate anche le politiche adottate in conformità ai principi di *privacy by design* e *privacy by default*.	--
Vengono seguiti standard e pratiche di codifica sicure.	--
Durante lo sviluppo, test e convalida viene eseguita l'implementazione dei requisiti di sicurezza iniziali.	--
Valutazione delle vulnerabilità, applicazione e test di penetrazione delle infrastrutture vengono eseguiti da una terza parte certificata prima dell'adozione operativa. L'applicazione considerata non dovrebbe poter essere adottata fino a quando non sia stato raggiunto il livello di sicurezza richiesto.	--
Vengono eseguiti test periodici di penetrazione.	Sì sono programmati

CATEGORIA DI APPARTENENZA DELLA MISURA DI SICUREZZA	PRESENTE (SI/NO) *Ove applicabile, motivare la scelta, dettagliando quanto possibile*
Vengono ottenuti informazioni sulle vulnerabilità tecniche dei sistemi informatici utilizzati.	--
I patch software vengono testati e valutati prima di essere installati in un ambiente operativo.	--
Sicurezza Fisica	
Il perimetro fisico dell'infrastruttura del sistema IT non è accessibile da personale non autorizzato.	E' all'interno di un armadio chiuso a chiave
Le zone sicure vengono definite e protette da appropriati controlli di accesso. Un registro fisico o una traccia elettronica di controllo di tutti gli accessi devono essere mantenuti e monitorati in modo sicuro.	Non presente
I sistemi di rilevamento antintrusione vengono installati in tutte le zone di sicurezza.	--
Se del caso, vengono costruite barriere fisiche per impedire l'accesso fisico non autorizzato.	Armadio chiuso
Un sistema antincendio automatico, un sistema di climatizzazione dedicato a controllo chiuso e un gruppo di continuità (UPS) vengono attivati nella sala server.	
Il personale di servizio di supporto esterno ha accesso limitato alle aree protette.	SI
Sicurezza su servizi in Cloud	
Gli elementi di sicurezza richiesti dai fornitori di servizi in Cloud rispettano le indicazioni fornite da più fonti, in riferimento a: - Affidabilità del fornitore *(esperienza, capacità e affidabilità del fornitore; caratteristiche della connettività; qualificazione del personale impiegato)*; - Portabilità dei dati *(sono ovviamente privilegiati i servizi che lo favoriscono)*; - Garanzie sulla disponibilità e sulle prestazioni dei servizi in cloud *(garanzie sulla riservatezza e sulla continuità operativa)*; - Dislocazione dei server ed eventuali dipendenze da altri fornitori; - Tempi e modalità di archiviazione e conservazione dei dati; - Tutele legali *(responsabilità, compliance, legge applicabile, foro competente)*.	Non ci sono servizi dati in cloud (a meno del pannello antivirus seqrite)