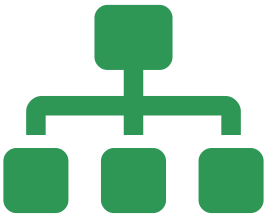
A.S.P. Cordenonese Virginia Fabbri Taliento



Registro dei trattamenti

Titolare del trattamento

Nome: A.S.P. Cordenonese Virginia Fabbri Taliento
Email: protocollo@aspcordenonese.it
Pec: aspcordenonese@pec.it
Telefono: 0434930440

Responsabile della protezione dati

Nome: Robyone SRL
Email: dpo@robyone.net
Pec: dpo.robyone@ronepec.it
Telefono: 0490998416

Via Cervel, 68 - 33084 Cordenons (PN)
Tel.: 0434930440 - Mail: protocollo@aspcordenonese.it - PEC: aspcordenonese@pec.it

Indice dei contenuti

Via Cervel, 68 - 33084 Cordenons (PN)
Tel.: 0434930440 - Mail: protocollo@aspcordenonese.it - PEC: aspcordenonese@pec.it

1 Acquisti

Finalità

Gestione di procedure di selezione del contraente per affidamento di servizi, beni e forniture , Stipula di contratti sotto forma di atto pubblico amministrativo, scrittura privata autenticata, scrittura privata scambio di lettere commerciali , Difesa di un diritto anche di un terzo in sede giudiziaria o amministrativa , Adempimento obblighi di legge

Categorie di interessati

Fornitori Esterni / Professionisti

Categorie di dati personali

Codice fiscale ed altri numeri di identificazione personale, Attività economiche, commerciali, finanziarie e assicurative, Beni, proprietà, possesso, compresi dati relativi al patrimonio immobiliare, Coordinate bancarie, Indirizzo e-mail e numero cellulare, Nominativo, indirizzo o altri elementi di identificazione personale, Dati genetici, Lavoro (occupazione attuale, precedente, curriculum, certificati di qualità professionali, ecc.), Informazioni di carattere giudiziario (GDPR 679/2016, art. 10)

Categorie di destinatari

Amministrativo Generico, Direttore, Fornitori Esterni / Professionisti, Fornitore Programmi Applicativi, Altre amministrazioni Pubbliche, Diffusione al pubblico

Termini ultimi previsti per la cancellazione

I dati sono conservati per un periodo non superiore a quello necessario al perseguimento della loro funzione. A tal fine, anche mediante controlli periodici, viene verificata costantemente la stretta pertinenza, non eccedenza e indispensabilità dei dati . I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non sono utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. I dati potranno essere conservati anche oltre il periodo di tempo necessario alle relative finalità, se ciò si renda necessario per fini di archiviazione nel pubblico interesse, di ricerca storica o a fini statistici, come previsto dall'art. 5 del Regolamento Europeo n. 679/2016

Via Cervel, 68 - 33084 Cordenons (PN)
Tel.: 0434930440 - Mail: protocollo@aspcordenonese.it - PEC: aspcordenonese@pec.it

2 Contabilità

Finalità

Gestione della contabilità utenti , Adempimenti fiscali e contabili nonché altri obblighi nascenti dalla normativa vigente , Adempimenti connessi al versamento delle quote di iscrizione a sindacati , Trattamento giuridico ed economico di personale, fornitori, Gestione del patrimonio mobiliare ed immobiliare, Monitoraggio degli adempimenti contrattuali

Categorie di interessati

Dipendenti, Fornitori Esterni / Professionisti, Clienti

Categorie di dati personali

Codice fiscale ed altri numeri di identificazione personale, Nominativo, indirizzo o altri elementi di identificazione personale, Attività economiche, commerciali, finanziarie e assicurative, Indirizzo e-mail e numero cellulare, Coordinate bancarie, Beni, proprietà, possesso, compresi dati relativi al patrimonio immobiliare, Informazioni di carattere giudiziario (GDPR 679/2016, art. 10), Dati relativi alla famiglia o a situazioni personali

Categorie di destinatari

Amministrativo Generico, Amministrativo Personale, Direttore, Fornitori Esterni / Professionisti, Fornitore Programmi Applicativi, Enti locali, Banche e istituti di credito, Altre amministrazioni Pubbliche, Organizzazioni sindacali e patronati, Imprese di assicurazione

Termini ultimi previsti per la cancellazione

I dati sono conservati per un periodo non superiore a quello necessario al perseguimento della loro funzione. A tal fine, anche mediante controlli periodici, viene verificata costantemente la stretta pertinenza, non eccedenza e indispensabilità dei dati . I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non sono utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. I dati potranno essere conservati anche oltre il periodo di tempo necessario alle relative finalità, se ciò si renda necessario per fini di archiviazione nel pubblico interesse, di ricerca storica o a fini statistici, come previsto dall'art. 5 del Regolamento Europeo n. 679/2016

Via Cervel, 68 - 33084 Cordenons (PN)
Tel.: 0434930440 - Mail: protocollo@aspcordenonese.it - PEC: aspcordenonese@pec.it

3 Gestione Immagini e Video

Finalità

Promozione dell'Ente con pubblicazione nei propri social media , Promozione delle attività dell'Ente con pubblicazione cartacee , Promozione delle attività dell'Ente con pubblicazione all'interno del sito internet istituzionale , Promozione delle attività dell'Ente con esposizione delle immagini all'interno dello stesso

Categorie di interessati

Dipendenti, Ospiti

Categorie di dati personali

Codice fiscale ed altri numeri di identificazione personale, Nominativo, indirizzo o altri elementi di identificazione personale, Immagini, Fotografie

Categorie di destinatari

Società di Servizi

Trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale

Facebook

Termini ultimi previsti per la cancellazione

"Le immagini e i video verranno conservati, per il tempo necessario alla loro funzione, nel rispetto del principio di minimizzazione enunciato all'art. 5 par 1 lett c Regolamento UE 2016/679 – GDPR. Il titolare verificherà, con cadenza periodica, l'obsolescenza dei dati resi pubblici e provvederà ad eliminare ogni contenuto risultante non più pertinente alla finalità per cui è stato pubblicato. Le foto di gruppo potranno essere conservate all'interno degli archivi dell'ente per finalità di documentazione storica"

Via Cervel, 68 - 33084 Cordenons (PN)
Tel.: 0434930440 - Mail: protocollo@aspcordenonese.it - PEC: aspcordenonese@pec.it

4 Inserimento Ospite CDR-CD

Finalità

Collaborazioni professionali esterne per adempimento degli obblighi di legge , Analisi statistiche anonime , Finalità amministrativo contabili legate alla gestione della richiesta , Presa in carico della richiesta di ingresso in struttura e gestione dell'eventuale successivo rapporto contrattuale , Adempimento obblighi di legge

Categorie di interessati

Familiari Firmatari, Ospiti, Familiari non Firmatari, Tutore - Amministratore di sostegno

Categorie di dati personali

Codice fiscale ed altri numeri di identificazione personale, Nominativo, indirizzo o altri elementi di identificazione personale, Dati relativi alla famiglia o a situazioni personali, Indirizzo e-mail e numero cellulare, Carte sanitarie, Stato di salute – patologie attuali, Stato di salute – patologie pregresse, Stato di salute – terapie in corso, Abitudini di vita e di consumo, Coordinate bancarie, Sesso (m/f), Stato di salute – anamnesi familiare, Stato di salute - altro, Fotografie, Professione religiosa

Categorie di destinatari

Personale ambito sanitario, Personale ambito socio - assistenziale, Fornitore Programmi Applicativi, Società di Servizi, Professionista ambito socio sanitario, Altre amministrazioni Pubbliche

Termini ultimi previsti per la cancellazione

I dati conferiti in sede di "domanda di ingresso", saranno conservati fino al perfezionamento della stessa e successivamente inseriti all'interno della cartella dell'ospite. Nel caso di mancato inserimento, i dati verranno conservati per un tempo non superiore ad anni cinque dal loro conferimento

Via Cervel, 68 - 33084 Cordenons (PN)
Tel.: 0434930440 - Mail: protocollo@aspcordenonese.it - PEC: aspcordenonese@pec.it

5 Gestione ospite CDR-CD

Finalità

Informazioni su iniziative organizzate e/o nuovi servizi erogati dall'Ente , Finalità amministrativo contabili connesse alla prestazione del servizio oggetto di contratto (programmazione, accettazione e contabilizzazione) , Assistenza socio-sanitaria dell'ospite , Prestare il servizio oggetto della richiesta di ingresso presentata ed altresì del successivo rapporto contrattuale stipulato con l'Ente, comprensivo di eventuali attività ricreative, occupazionali e/o sportive organizzate dallo stesso con il possibile coinvolgimento di associazioni di volontariato , Analisi statistiche anonime , Adempimento obblighi di legge

Categorie di interessati

Familiari Firmatari, Ospiti, Familiari non Firmatari, Tutore - Amministratore di sostegno

Categorie di dati personali

Codice fiscale ed altri numeri di identificazione personale, Nominativo, indirizzo o altri elementi di identificazione personale, Sesso (m/f), Carte sanitarie, Stato di salute – patologie attuali, Stato di salute – patologie pregresse, Stato di salute – terapie in corso, Stato di salute – anamnesi familiare, Vita sessuale, Fotografie, Professione religiosa, Stato di salute - altro, Dati relativi alla famiglia o a situazioni personali, Abitudini di vita e di consumo, Coordinate bancarie, Indirizzo e-mail e numero cellulare

Categorie di destinatari

Personale ambito sanitario, Personale ambito socio - assistenziale, Fornitore Programmi Applicativi, Società di Servizi, Professionista ambito socio sanitario, Altre amministrazioni Pubbliche

Termini ultimi previsti per la cancellazione

I dati conferiti saranno conservati fino alla conclusione del contratto e, successivamente, per il tempo necessario all'espletamento della loro funzione, nel rispetto del principio di minimizzazione disciplinato dall'articolo 5 par. 1 lett. c del Regolamento UE 2016/679 – GDPR. I dati contenuti all'interno della cartella clinica dell'interessato saranno conservati illimitatamente, così come stabilito nella circolare del Ministero della Sanità n.900 2/AG454/260, emanata il 19 dicembre 1986

Via Cervel, 68 - 33084 Cordenons (PN)
Tel.: 0434930440 - Mail: protocollo@aspcordenonese.it - PEC: aspcordenonese@pec.it

6 Reclutamento

Finalità

Finalità amministrativo contabili nella fase antecedente all'eventuale sottoscrizione del contratto di lavoro o collaborazione , Gestione del procedimento di selezione del personale e/o di collaboratori nonché prosecuzione di eventuali trattative in fase precontrattuale , Difesa di un diritto anche di un terzo in sede giudiziaria o amministrativa , Adempimento obblighi di legge

Categorie di interessati

Autorizzato al trattamento, Dipendenti, Direttore, Consiglio di Amministrazione, Tirocinanti , Candidati

Categorie di dati personali

Codice fiscale ed altri numeri di identificazione personale, Nominativo, indirizzo o altri elementi di identificazione personale, Lavoro (occupazione attuale, precedente, curriculum, certificati di qualità professionali, ecc.), Istruzione, Indirizzo e-mail e numero cellulare, Dati genetici, Idoneità al lavoro, Fotografie, Dati relativi alla famiglia o a situazioni personali, Coordinate bancarie, Sesso (m/f), Informazioni di carattere giudiziario (GDPR 679/2016, art. 10), Iscrizione a sindacato

Categorie di destinatari

Autorizzato al trattamento, Dipendenti, Direttore, Consiglio di Amministrazione, Tirocinanti , Candidati

Termini ultimi previsti per la cancellazione

I dati verranno conservati per il tempo minimo necessario alla loro funzione e comunque per un periodo massimo di mesi 18 dalla loro raccolta salvo la conservazione per un periodo successivo in caso di eventuali contenzioni, richieste delle autorità competenti o ai sensi della vigente normativa

Via Cervel, 68 - 33084 Cordenons (PN)
Tel.: 0434930440 - Mail: protocollo@aspcordenonese.it - PEC: aspcordenonese@pec.it

7 Gestione risorse umane

Finalità

Difesa di un diritto anche di un terzo in sede giudiziaria o amministrativa , Adempimento obblighi di legge, Gestione obblighi ex D.lgs.81\2008 , Gestione periodi di malattia e istanze ai sensi di L. 104\1992 e D.lgs. 151\2001 , Gestione dati per finalità pensionistiche ed assistenziali , Organizzazione interna e gestione delle risorse , Gestione di ferie e permessi , Tenuta della contabilità e della corresponsione di emolumenti e\o benefici nonché riconoscimento di agevolazioni e erogazione di contributi , Gestione dell'assunzione presso l'Ente anche con i dati forniti in fase concorsuale, e gestione, esecuzione ed estinzione del rapporto lavorativo con l'Ente

Categorie di interessati

Ruoli privacy, Dipendenti, Direttore, Consiglio di Amministrazione, LPU - Lavoratori di Pubblica Utilità, Tirocinanti , Destinatari trattamenti, Candidati

Categorie di dati personali

Nominativo, indirizzo o altri elementi di identificazione personale, Lavoro (occupazione attuale, precedente, curriculum, certificati di qualità professionali, ecc.), Istruzione, Indirizzo e-mail e numero cellulare, Idoneità al lavoro, Informazioni di carattere giudiziario (GDPR 679/2016, art. 10), Codice fiscale ed altri numeri di identificazione personale, Dati sul comportamento, profili di utenti, consumatori, contribuenti, ecc., Stato di salute - altro, Carte sanitarie, Dati relativi alla famiglia o a situazioni personali, Coordinate bancarie

Categorie di destinatari

Dipendenti, Direttore, Consiglio di Amministrazione, LPU - Lavoratori di Pubblica Utilità, Tirocinanti , Destinatari trattamenti, Candidati

Termini ultimi previsti per la cancellazione

I dati del dipendente verranno conservati per il tempo minimo necessario alla loro funzione, nel rispetto del principio di minimizzazione dei dati imposto dall'art.5 par.1 lett.c del GDPR. In particolare, essi verranno conservati per tutta la durata del rapporto tra le parti e, successivamente, nei limiti derivati da obblighi di legge in materia amministrativa, contrattuale e fiscale. I dati del dipendente potrebbero richiedere un periodo di conservazione superiore in caso di controversie pendenti.

Via Cervel, 68 - 33084 Cordenons (PN)
Tel.: 0434930440 - Mail: protocollo@aspcordenonese.it - PEC: aspcordenonese@pec.it

8 Gestione tirocinanti-stagisti

Finalità

Organizzazione del servizio erogato , Gestione delle presenze , Instaurazione e gestione del rapporto di collaborazione , Difesa di un diritto anche di un terzo in sede giudiziaria o amministrativa , Adempimento obblighi di legge

Categorie di interessati

Tirocinanti

Categorie di dati personali

Codice fiscale ed altri numeri di identificazione personale, Nominativo, indirizzo o altri elementi di identificazione personale, Istruzione, Indirizzo e-mail e numero cellulare, Stato di salute - altro

Categorie di destinatari

Dipendenti, Società di Servizi, Professionista ambito socio sanitario

Termini ultimi previsti per la cancellazione

I dati dell'interessato verranno conservati per il tempo minimo necessario alla loro funzione, nel rispetto del principio di minimizzazione del trattamento dei dati imposto dall'art. 5 par. 1 lett. c del GDPR. In particolare, essi verranno conservati per tutta la durata del rapporto tra le parti e, successivamente, nei limiti derivati dagli obblighi di legge in materia amministrativa, contrattuale, contabile e fiscale

Via Cervel, 68 - 33084 Cordenons (PN)
Tel.: 0434930440 - Mail: protocollo@aspcordenonese.it - PEC: aspcordenonese@pec.it

9 Gestione emergenza COVID

Finalità

Gestire l'emergenza sanitaria da COVID-19

Categorie di interessati

Dipendenti, Fornitori Esterni / Professionisti, Familiari Firmatari, Tirocinanti , Familiari non Firmatari, Tutore - Amministratore di sostegno

Categorie di dati personali

Nominativo, indirizzo o altri elementi di identificazione personale, Lavoro (occupazione attuale, precedente, curriculum, certificati di qualità professionali, ecc.), Stato di salute - altro

Categorie di destinatari

Dipendenti, Società di Servizi, Altre amministrazioni Pubbliche

Termini ultimi previsti per la cancellazione

Fino al termine dell'emergenza sanitaria, salvo contenzioso

Via Cervel, 68 - 33084 Cordenons (PN)
Tel.: 0434930440 - Mail: protocollo@aspcordenonese.it - PEC: aspcordenonese@pec.it

10 Gestione LPU

Finalità

Instaurazione e gestione dell'attività non retribuita presso l'Ente ai sensi del decreto ministeriale 26 marzo 2001, Organizzazione del servizio erogato , Gestione delle presenze , Difesa di un diritto anche di un terzo in sede giudiziaria o amministrativa , Gestione obblighi ex D.lgs.81\2008 , Gestione periodi di malattia e istanze ai sensi di L. 104\1992 e D.lgs. 151\2001 , Organizzazione interna e gestione delle risorse , Gestione di ferie e permessi

Categorie di interessati

LPU - Lavoratori di Pubblica Utilità

Categorie di dati personali

Codice fiscale ed altri numeri di identificazione personale, Nominativo, indirizzo o altri elementi di identificazione personale, Indirizzo e-mail e numero cellulare, Informazioni di carattere giudiziario (GDPR 679/2016, art. 10)

Categorie di destinatari

Amministrativo Generico, Direttore, Personale ambito socio - assistenziale, Società di Servizi

Termini ultimi previsti per la cancellazione

I dati personali e particolari verranno conservati per il tempo minimo necessario alla loro funzione, nel rispetto del principio di minimizzazione del trattamento dei dati imposto dall'art. 5 par. 1 lett. c del GDPR. In particolare, essi verranno conservati per tutta la durata del rapporto tra le parti e, successivamente, nei limiti derivati dagli obblighi di legge in materia amministrativa e contrattuale

11 Descrizione generale delle misure di sicurezza tecniche e organizzative

- **Accesso alle reti e ai servizi di rete**
  Agli utenti devono essere forniti solo degli accesi alle reti ed ai servizi di rete per il cui uso sono stati specificatamente autorizzati
- **Accordi di riservatezza o di non divulgazione**
  I requisiti per gli accordi di riservatezza o di non divulgazione che riflettono le necessità dell'organizzazione per la protezione delle informazioni devono essere identificati, riesaminati periodicamente e documentati
- **Accordi per il trasferimento delle informazioni**
  I trasferimenti sicuri di informazioni di business tra l'organizzazione e le parti esterne devono essere indirizzati in appositi accordi
- **Analisi e specifica dei requisiti per la sicurezza delle informazioni**
  I requisiti relativi alla sicurezza delle informazioni devono essere inclusi all'interno dei requisiti per i nuovi sistemi informativi o per l'aggiornamento di quelli esistenti. Include il controllo dei file temporanei.
- **Apparecchiature incustodite degli utenti**
  Gli utenti devono assicurare che le apparecchiature incustodite siano appropriatamente protette
- **Apprendimento dagli incidenti relativi alla sicurezza delle informazioni**
  La conoscenza acquisita dall'analisi e dalla soluzione degli incidenti relativi alla sicurezza delle informazioni deve essere utilizzata per ridurre la verosimiglianza o l'impatto degli incidenti futuri
- **Attuazione della continuità della sicurezza delle informazioni**
  L'organizzazione deve stabilire, documentare, attuare e mantenere processi, procedure e controlli per assicurare il livello di continuità richiesto per la sicurezza delle informazioni durante una situazione avversa
- **Backup delle informazioni**
  Devono essere effettuate copie di backup delle informazioni, del software e delle immagini dei sistemi e quindi sottoposte a test periodici secondo una politica di backup concordata

Via Cervel, 68 - 33084 Cordenons (PN)
Tel.: 0434930440 - Mail: protocollo@aspcordenonese.it - PEC: aspcordenonese@pec.it

- **Cessazione o variazione delle responsabilità durante il rapporto di lavoro**
  Le responsabilità e i doveri relativi alla sicurezza delle informazioni che rimangono validi dopo la cessazione o la variazione del rapporto di lavoro devono essere definiti, comunicati al personale o al collaboratore e resi effettivi
- **Classificazione delle informazioni**
  Le informazioni devono essere classificate in relazione al loro valore, ai requisiti cogenti e alla criticità in caso di divulgazione o modifica non autorizzate
- **Consapevolezza, istruzione, formazione e addestramento sulla sicurezza delle informazioni**
  Tutto il personale dell'organizzazione e, quando pertinente, il collaboratore, devono ricevere un'adeguata sensibilizzazione, istruzione, formazione e addestramento e aggiornamenti periodici sulle politiche e procedure organizzative, in modo pertinente alla loro attività lavorativa
- **Contatti con gruppi specialistici**
  Devono essere mantenuti appropriati contatti con gruppi specialistici o altri contesti ed associazioni professionali frequentate da specialisti della sicurezza delle informazioni
- **Contatti con le autorità**
  Devono essere mantenuti appropriati contatti con le autorità pertinenti
- **Controlli contro il malware**
  Devono essere attuati controlli di individuazione, di prevenzione e di ripristino relativamente al malware, congiuntamente ad un'appropriata consapevolezza degli utenti
- **Controlli di rete**
  Le reti devono essere gestite e controllate per proteggere le informazioni nei sistemi e nelle applicazioni. Firewall, VLAN, eccetera.
- **Controlli per l'audit dei sistemi informativi**
  I requisiti e le attività di audit che prevedono una verifica dei sistemi di produzione devono essere attentamente pianificati e concordati per minimizzare le interferenze con i processi di business
- **Diritti di proprietà intellettuale**
  Devono essere attuate delle procedure adeguate a garantire la conformità ai requisiti cogenti e contrattuali per l'uso del materiale sul quale potrebbero insistere diritti di proprietà intellettuale e per l'uso di prodotti software proprietari
- **Disponibilità delle strutture per l'elaborazione delle informazioni**
  Le strutture per l'elaborazione delle informazioni devono essere realizzate con una ridondanza sufficiente a soddisfare i requisiti di disponibilità
- **Etichettatura delle informazioni**
  Deve essere sviluppato e attuato un appropriato insieme di procedure per l'etichettatura delle informazioni in base allo schema di classificazione adottato dall'organizzazione
- **Filiera di fornitura per l'ICT (Information and communication technology)**
  Gli accordi con i fornitori devono includere i requisiti per affrontare i rischi relativi alla sicurezza delle informazioni associati ai servizi e ai prodotti della filiera di fornitura per l'ICT
- **Gestione degli incidenti: Responsabilità e procedure**
  Devono essere stabilite le responsabilità e le procedure di gestione per assicurare una risposta rapida, efficace ed ordinata agli incidenti relativi alla sicurezza delle informazioni
- **Gestione dei cambiamenti (sistemistici)**
  I cambiamenti all'organizzazione, ai processi di business, alle strutture di elaborazione delle informazioni e ai sistemi che influenzano la sicurezza delle informazioni devono essere controllati.
- **Gestione dei cambiamenti ai servizi dei fornitori**
  I cambiamenti alla fornitura dei servizi da parte dei fornitori, incluso il mantenimento e il miglioramento delle attuali politiche, procedure e controlli per la sicurezza delle informazioni, devono essere gestiti, tenendo conto della criticità delle informazioni di business, dei sistemi e processi coinvolti e della rivalutazione dei rischi
- **Gestione dei diritti di accesso privilegiato**
  L'assegnazione e l'uso di diritti di accesso privilegiato devono essere limitati e controllati
- **Gestione dei supporti rimovibili**
  Devono essere sviluppate procedure per il trattamento dei supporti rimovibili in base allo schema di classificazione adottato dall'organizzazione

Via Cervel, 68 - 33084 Cordenons (PN)
Tel.: 0434930440 - Mail: protocollo@aspcordenonese.it - PEC: aspcordenonese@pec.it

- **Gestione della capacità**
  L'uso delle risorse deve essere monitorato e messo a punto. Si devono fare proiezioni sui futuri requisiti di capacità per assicurare le prestazioni di sistema richieste
- **Gestione delle chiavi**
  Deve essere sviluppata e attuata una politica sull'uso, sulla protezione e sulla durata delle chiavi crittografiche attraverso il loro intero ciclo di vita
- **Gestione delle informazioni segrete di autenticazione degli utenti**
  L'assegnazione di informazioni segrete di autenticazione deve essere controllata attraverso un processo di gestione formale. Ossia: Gestione delle password (o PIN o passphrase) degli utenti.
- **Gestione delle vulnerabilità tecniche**
  Le informazioni sulle vulnerabilità tecniche dei sistemi informativi utilizzati devono essere ottenute in modo tempestivo, l'esposizione a tali vulnerabilità deve essere valutata e appropriate misure devono essere intraprese per affrontare i rischi relativi. Patching
- **Identificazione della legislazione applicabile e dei requisiti contrattuali**
  Per ogni sistema informativo e per l'organizzazione in generale si devono esplicitamente definire, documentare e mantenere aggiornati tutti i requisiti cogenti e contrattuali pertinenti, oltre all'approccio stesso dell'organizzazione per soddisfarli
- **Indirizzare la sicurezza all'interno degli accordi con i fornitori**
  Tutti i requisiti relativi alla sicurezza delle informazioni devono essere stabiliti e concordati con ciascun fornitore che potrebbe avere accesso, elaborare, archiviare, trasmettere o fornire componenti dell'infrastruttura IT per le informazioni dell'organizzazione
- **Infrastrutture di supporto**
  Le apparecchiature devono essere protette da malfunzionamenti alla rete elettrica di alimentazione e da altri disservizi causati da malfunzionamenti dei servizi ausiliari
- **Lavoro in aree sicure**
  Devono essere progettate e attuate procedure per lavorare nelle aree sicure
- **Limitazione dell'accesso alle informazioni**
  L'accesso a informazioni e funzioni di sistemi applicativi deve essere limitato secondo le politiche di controllo degli accessi
- **Limitazioni ai cambiamenti dei pacchetti software**
  La modifica dei pacchetti software deve essere disincentivata e limitata ai cambiamenti necessari; inoltre, tutti i cambiamenti devono essere strettamente controllati
- **Limitazioni all'installazione del software**
  Devono essere stabilite e attuate regole per il governo dell'installazione del software da parte degli utenti
- **Log di amministratori e operatori**
  Le attività degli amministratori e degli operatori di sistema devono essere sottoposte a log, e questi devono essere protetti e riesaminati periodicamente
- **Manutenzione delle apparecchiature**
  Le apparecchiature devono essere correttamente mantenute per assicurare la loro continua disponibilità e integrità
- **Messaggistica elettronica**
  Le informazioni trasmesse attraverso messaggistica elettronica devono essere protette in modo appropriato
- **Monitoraggio e riesame dei servizi dei fornitori**
  Le organizzazioni devono regolarmente monitorare, riesaminare e sottoporre a audit l'erogazione dei servizi da parte dei fornitori
- **Pianificazione della continuità della sicurezza delle informazioni**
  L'organizzazione deve determinare i propri requisiti per la sicurezza delle informazioni e per la continuità della gestione della sicurezza delle informazioni in situazioni avverse, per esempio durante crisi o disastri
- **Politica di controllo degli accessi**
  Una politica di controllo degli accessi deve essere definita, documentata ed aggiornata sulla base dei requisiti di business e di sicurezza delle informazioni
- **Politica di schermo e scrivania puliti**
  Devono essere adottate sia una politica di "scrivania pulita" per i documenti ed i supporti di memorizzazione rimovibili, sia una politica di "schermo pulito" per i servizi di elaborazione delle informazioni
- **Politica per la sicurezza delle informazioni nei rapporti con i fornitori**
  I requisiti di sicurezza delle informazioni per mitigare i rischi associati all'accesso agli asset dell'organizzazione da parte dei fornitori devono essere concordati con i fornitori stessi e documentati

Via Cervel, 68 - 33084 Cordenons (PN)
Tel.: 0434930440 - Mail: protocollo@aspcordenonese.it - PEC: aspcordenonese@pec.it

- **Politica sull'uso dei controlli crittografici**
  Deve essere sviluppata e attuata una politica sull'uso dei controlli crittografici per la protezione delle informazioni. Per i dati sui server e sui database, per i pc e i dispositivi portatili (p.e. smartphone e tablet), per le memorie rimovibili (p.e. chiavi USB), per la trasmissione.
- **Politiche e procedure per il trasferimento delle informazioni**
  Devono esistere politiche, procedure e controlli formali a protezione del trasferimento delle informazioni attraverso l'uso di tutte le tipologie di strutture di comunicazione
- **Politiche per la sicurezza delle informazioni**
  Un insieme di politiche per la sicurezza delle informazioni deve essere definito, approvato dalla direzione, pubblicato e comunicato al personale e alle parti esterne pertinenti
- **Principi per l'ingegnerizzazione sicura dei sistemi**
  I principi per l'ingegnerizzazione di sistemi sicuri devono essere stabiliti, documentati, manutenuti e applicati ad ogni iniziativa di implementazione di un sistema informativo
- **Privacy e protezione dei dati personali**
  Si devono assicurare la privacy e la protezione dei dati personali, come richiesto dalla legislazione e dai regolamenti pertinenti, per quanto applicabile
- **Procedure di log-on sicure**
  Quando richiesto dalle politiche di controllo degli accessi, l'accesso a sistemi e applicazioni deve essere controllato da procedure di log-on sicure
- **Procedure operative documentate**
  Devono essere documentate e rese disponibili delle procedure operative a tutti gli utenti che le necessitano
- **Procedure per il controllo dei cambiamenti di sistema**
  I cambiamenti ai sistemi all'interno del ciclo di vita devono essere tenuti sotto controllo attraverso l'utilizzo di procedure formali di controllo dei cambiamenti
- **Processo disciplinare**
  Deve essere istituito un processo disciplinare, formale e comunicato, per intraprendere provvedimenti nei confronti del personale che ha commesso una violazione della sicurezza delle informazioni
- **Protezione delle informazioni di log**
  Le strutture per la raccolta dei log e le informazioni di log devono essere protette da manomissioni e accessi non autorizzati
- **Protezione delle registrazioni**
  Le registrazioni devono essere protette da perdita, distruzione, falsificazione, accesso non autorizzato e rilascio non autorizzato in conformità ai requisiti cogenti, contrattuali e di business
- **Provisioning degli accessi degli utenti**
  Deve essere attuato un processo formale per l'assegnazione o la revoca dei diritti di accesso per tutte le tipologie di utenze e per tutti i sistemi e servizi
- **Raccolta di evidenze**
  L'organizzazione deve definire ed applicare opportune procedure per l'identificazione, la raccolta, l'acquisizione e la conservazione delle informazioni che possono essere impiegate come evidenze
- **Raccolta di log degli eventi (e monitoraggio)**
  La registrazione dei log degli eventi, delle attività degli utenti, delle eccezioni, dei malfunzionamenti e degli eventi relativi alla sicurezza delle informazioni deve essere effettuata, mantenuta e riesaminata periodicamente
- **Registrazione e de-registrazione degli utenti**
  Deve essere attuato un processo formale di registrazione e de-registrazione per abilitare l'assegnazione dei diritti di accesso
- **Rendere sicuri uffici, locali e strutture**
  Deve essere progettata e applicata la sicurezza fisica agli uffici, ai locali ed agli impianti. Inclusi armadi (archivi) per i documenti cartacei.
- **Responsabilità degli asset**
  Gli asset censiti nell'inventario devono avere un responsabile
- **Responsabilità della direzione**
  La direzione deve richiedere a tutto il personale e ai collaboratori di applicare la sicurezza delle informazioni in conformità con le politiche e le procedure stabilite dall'organizzazione

Via Cervel, 68 - 33084 Cordenons (PN)
Tel.: 0434930440 - Mail: protocollo@aspcordenonese.it - PEC: aspcordenonese@pec.it

- **Restituzione degli asset**
  Tutto il personale e gli utenti di parti esterne devono restituire tutti gli asset dell'organizzazione in loro possesso al termine del periodo di impiego, del contratto o dell'accordo stipulato
- **Riesame dei diritti di accesso degli utenti**
  I responsabili degli asset devono riesaminare ad intervalli regolari i diritti di accesso degli utenti
- **Riesame delle politiche per la sicurezza delle informazioni**
  Le politiche per la sicurezza delle informazioni devono essere riesaminate ad intervalli pianificati o nel caso in cui si siano verificati cambiamenti significativi, al fine di garantirne sempre l'idoneità, l'adeguatezza e l'efficacia.
- **Rimozione o adattamento dei diritti di accesso**
  I diritti di accesso di tutto il personale e degli utenti di parti esterne a informazioni e strutture di elaborazione delle informazioni devono essere rimossi al momento della cessazione del rapporto di lavoro, del contratto o accordo, oppure adattate ad ogni variazione
- **Risposta agli incidenti relativi alla sicurezza delle informazioni**
  Si deve rispondere agli incidenti relativi alla sicurezza delle informazioni in accordo alle procedure documentate
- **Ruoli e responsabilità per la sicurezza delle informazioni**
  Tutte le responsabilità relative alla sicurezza delle informazioni dovrebbero essere definite e assegnate
- **Screening**
  Devono essere svolti dei controlli per la verifica del background effettuati su tutti i candidati all'impiego in accordo con le leggi, con i regolamenti pertinenti e con l'etica e devono essere proporzionati alle esigenze di business, alla classificazione delle informazioni da accedere e ai rischi percepiti
- **Segnalazione degli eventi relativi alla sicurezza delle informazioni**
  Gli eventi relativi alla sicurezza delle informazioni devono essere segnalati il più velocemente possibile attraverso appropriati canali gestionali
- **Segregazione nelle reti**
  Nelle reti si devono segregare gruppi di servizi, di utenti e di sistemi informativi
- **Separazione dei compiti**
  I compiti e le aree di responsabilità in conflitto tra loro devono essere separati per ridurre le possibilità di uso improprio, modifica non autorizzata o non intenzionale degli asset dell'organizzazione
- **Sicurezza dei cablaggi**
  I cavi per l'energia elettrica e le telecomunicazioni adibiti al trasporto di dati o a supporto di servizi informativi devono essere protetti da intercettazioni, interferenze o danneggiamenti
- **Sicurezza dei servizi applicativi su reti pubbliche**
  Le informazioni coinvolte nei servizi applicativi che transitano su reti pubbliche devono essere protette da attività fraudolente, da dispute contrattuali, da divulgazioni e da modifiche non autorizzate
- **Sicurezza dei servizi di rete**
  I meccanismi di sicurezza, i livelli di servizio e i requisiti di gestione di tutti i servizi di rete devono essere identificati e inclusi negli accordi sui livelli di servizio relativi alla rete, indipendentemente dal fatto che tali servizi siano forniti dall'interno o siano affidati all'esterno
- **Sicurezza delle informazioni nella gestione dei progetti**
  La sicurezza delle informazioni deve essere indirizzata nell'ambito della gestione dei progetti, a prescindere dal tipo di progetto
- **Sincronizzazione degli orologi**
  Gli orologi di tutti i sistemi pertinenti che elaborano informazioni all'interno di un'organizzazione o di un dominio di sicurezza devono essere sincronizzati rispetto a una singola sorgente temporale di riferimento
- **Sistema di gestione delle password**
  I sistemi di gestione delle password devono essere interattivi e devono assicurare password di qualità
- **Termini e condizioni di impiego**
  Gli accordi contrattuali con il personale e con i collaboratori devono specificare le responsabilità loro e dell'organizzazione relativamente alla sicurezza delle informazioni
- **Trasporto dei supporti fisici**
  I supporti che contengono informazioni devono essere protetti da accessi non autorizzati, utilizzi impropri o manomissioni durante il trasporto

Via Cervel, 68 - 33084 Cordenons (PN)
Tel.: 0434930440 - Mail: protocollo@aspcordenonese.it - PEC: aspcordenonese@pec.it

- **Trattamento degli asset**
  Deve essere sviluppato e attuato un insieme di procedure per il trattamento degli asset in base allo schema di classificazione adottato dall'organizzazione
- **Uso di programmi di utilità privilegiati**
  L'uso di programmi di utilità che potrebbero essere in grado di aggirare i controlli applicativi e di sistema deve essere limitato e strettamente controllato
- **Utilizzo accettabile degli asset**
  Le regole per l'utilizzo accettabile delle informazioni e degli asset associati alle strutture di elaborazione delle informazioni devono essere identificate, documentate e attuate. Regole al personale anche relative a: uso dei dispositivi portatili, BYOD, scrivania pulita, schermo pulito, trasporto (p.e. dei documenti cartacei), blocco dei pc quando non usati, eccetera.
- **Utilizzo delle informazioni segrete di autenticazione**
  Gli utenti devono essere tenuti a seguire le prassi dell'organizzazione nell'uso di informazioni segrete di autenticazione
- **Valutazione e decisione sugli eventi relativi alla sicurezza delle informazioni**
  Gli eventi relativi alla sicurezza devono essere valutati e deve essere deciso se classificarli come incidenti relativi alla sicurezza delle informazioni
- **Verifica, riesame e valutazione della continuità della sicurezza delle informazioni**
  L'organizzazione deve verificare ad intervalli di tempo regolari i controlli di continuità della sicurezza delle informazioni stabiliti e attuati, al fine di assicurare che siano validi ed efficaci durante situazioni avverse