D.O.C. s.c.s., ai sensi della legge 381/91, è una cooperativa sociale di tipo A che pone al centro della propria crescita organizzativa i valori cooperativi della centralità della persona, della solidarietà, della partecipazione e dell'educazione.

Attiva dal 1988 nel settore del turismo sociale, D.O.C. ha maturato un'esperienza significativa nella gestione di strutture ricettive e nella progettazione di servizi educativi per minori, oltre a iniziative in ambito ambientale, culturale e di housing sociale. La cooperativa si configura oggi come un vero e proprio "sistema esperto" capace di tradurre competenze in pratiche trasferibili e orientate alla cittadinanza attiva.

Consapevole della delicatezza dei servizi erogati e dell'importanza della tutela delle informazioni, D.O.C. s.c.s. ha deciso di adottare una policy strutturata per la sicurezza informatica, in coerenza con i propri valori fondanti e in pieno rispetto delle normative europee sulla protezione dei dati personali, in particolare del Regolamento (UE) 2016/679 (GDPR)

La presente policy stabilisce le linee guida per proteggere le informazioni e i sistemi informatici aziendali. Include le disposizioni del Regolamento (UE) 2016/679 (GDPR), in particolare in materia di violazione dei dati personali (Data Breach) e gestione delle richieste da parte degli interessati.

AMBITO DI APPLICAZIONE

Si applica a tutti i dipendenti, collaboratori, fornitori e terzi che accedono ai sistemi informatici di D.O.C. s.c.s., in sede o da remoto.

RESPONSABILITÀ

Responsabile IT e Privacy Manager

Il Responsabile IT, congiuntamente al Privacy Manager, ha il compito di esercitare una supervisione generale sulle attività relative alla sicurezza delle informazioni e alla protezione dei dati personali. Tra le sue responsabilità rientra anche la gestione degli eventuali casi di violazione, garantendo una risposta tempestiva ed efficace a qualsiasi incidente.

DPO (Data Protection Officer)

Ha il ruolo di monitorare in maniera costante la conformità dell'organizzazione alle normative in materia di privacy. Il suo intervento è fondamentale per assicurare che i trattamenti dei dati personali siano effettuati nel rispetto delle disposizioni legislative vigenti.

RGQ (Responsabile Gestione Qualità)

Ha il compito di coordinare l'implementazione, il mantenimento e il miglioramento continuo del sistema di gestione della sicurezza delle informazioni. Questo ruolo assicura che le misure di sicurezza adottate siano efficaci, aggiornate e coerenti con gli obiettivi dell'organizzazione.

I soci e tutto il personale

Tutti i soci e in generale il personale di D.O.C. s.c.s. sono tenuti a rispettare integralmente quanto previsto dalla presente policy. Hanno inoltre l'obbligo di segnalare tempestivamente qualsiasi

anomalia, sospetto di violazione o comportamento non conforme alle regole di sicurezza e privacy, contribuendo così in modo attivo alla protezione delle informazioni e dei dati trattati dall'organizzazione.

GESTIONE DEGLI ACCESSI

L'accesso ai sistemi informativi aziendali è consentito esclusivamente tramite account personali, ciascuno associato a credenziali univoche. Le password devono essere complesse, rispondere ai requisiti minimi di sicurezza stabiliti e devono essere aggiornate con cadenza regolare.

L'accesso alle informazioni e alle risorse aziendali è regolato dal principio del "minimo privilegio", il quale prevede che ciascun utente possa accedere solo ai dati strettamente necessari allo svolgimento delle proprie mansioni.

UTILIZZO DEI DISPOSITIVI

È severamente vietato installare software non autorizzato sui dispositivi aziendali. Tutti i dispositivi devono essere protetti da soluzioni antivirus e firewall aggiornati e configurati in modo adeguato. Inoltre, i dispositivi forniti dall'organizzazione devono essere utilizzati esclusivamente per finalità lavorative, in linea con le policy aziendali.

SICUREZZA DELLA POSTA ELETTRONICA E NAVIGAZIONE

Gli utenti devono prestare particolare attenzione nell'utilizzo della posta elettronica, evitando di cliccare su link sospetti o aprire allegati provenienti da mittenti non attendibili. L'utilizzo dell'e-mail aziendale per scopi personali deve essere limitato e comunque conforme alle norme interne. La navigazione internet è consentita solo su siti ritenuti sicuri e pertinenti all'attività lavorativa.

FORMAZIONE E SIMULAZIONI DI PHISHING

Per aumentare la consapevolezza e la preparazione del personale in materia di sicurezza informatica, l'organizzazione prevede simulazioni periodiche di attacchi phishing. Inoltre, è obbligatoria una sessione annuale di formazione per tutti i dipendenti, finalizzata a rafforzare le competenze in tema di cybersecurity. I risultati delle simulazioni vengono analizzati per individuare eventuali criticità e definire misure correttive.

BACKUP E RECUPERO DATI

D.O.C. provvede a backup regolari dei dati aziendali, con modalità che ne garantiscano la cifratura e la sicurezza. I backup sono conservati in luoghi protetti, sia fisici che virtuali, per garantirne l'integrità e la disponibilità in caso di necessità di ripristino.

GESTIONE DELLE VIOLAZIONI DEI DATI (DATA BREACH)

Una violazione dei dati, o *Data Breach*, è definita in conformità con quanto previsto dal Regolamento Generale sulla Protezione dei Dati (GDPR). In caso di incidente, le figure coinvolte nella gestione sono il Delegato Privacy, il DPO, se designato, e l'ICT Manager.

È previsto l'obbligo di segnalazione dell'evento entro 72 ore dalla sua scoperta. Tutte le violazioni devono essere documentate nel Registro delle Violazioni dei Dati (RVD), includendo dettagli sull'accaduto, azioni intraprese e risultati ottenuti.
Devono essere adottate tempestivamente tutte le contromisure necessarie a contenere l'incidente. È inoltre prevista una valutazione del rischio che può, se necessario, comportare la notifica al Garante per la Protezione dei Dati Personali e agli interessati.

DIRITTI DEGLI INTERESSATI

D.O.C. garantisce la gestione conforme di tutte le richieste da parte degli interessati in materia di privacy, compresi i diritti di accesso, rettifica, cancellazione, opposizione e portabilità dei dati.
Le richieste devono ricevere risposta entro 30 giorni dalla ricezione e devono essere tracciate nel Registro delle Richieste e Comunicazioni con l'Interessato (RRCI).
Tutte le comunicazioni con gli interessati devono essere redatte in modo chiaro, trasparente e tempestivo.

SANZIONI

La violazione della presente policy comporta l'applicazione di sanzioni disciplinari, secondo quanto previsto dai regolamenti aziendali e, nei casi più gravi, può dar luogo ad azioni legali. Le misure sanzionatorie sono proporzionate alla gravità della violazione.

VERIFICHE E AUDIT

L'efficacia delle procedure previste dalla policy viene verificata attraverso audit annuali, che permettono di valutare il rispetto delle normative e delle buone pratiche.
Tali audit devono essere documentati in modo dettagliato e svolti secondo il ciclo di miglioramento continuo PDCA (Plan-Do-Check-Act).

REVISIONE DELLA POLICY

La presente policy è soggetta a revisione almeno una volta all'anno oppure in caso di aggiornamenti normativi, tecnologici o organizzativi rilevanti. Ogni revisione deve essere documentata, tracciata e formalmente approvata dal management, assicurando che le modifiche siano comunicate a tutto il personale coinvolto.

CONCLUSIONI

D.O.C. s.c.s. si impegna affinché ogni singolo socio e collaboratore venga messo nelle condizioni di comprendere appieno gli obiettivi della presente policy e di partecipare attivamente al loro raggiungimento attraverso le mansioni affidate. Ciascuno è chiamato a diventare protagonista consapevole e responsabile del livello di qualità, della tutela dei dati e della sicurezza nello svolgimento delle proprie attività, acquisendo e aggiornando costantemente le competenze necessarie per un'azione professionale sicura, efficace e coerente con i valori della cooperativa.

Il Consiglio di Amministrazione - D.O.C. s.c.s.