Via Valdagno 41
33100 Udine UD Italy
Cap. Soc. € 50.000,00 i.v.
T +39 0432 741160
F +39 0432 741162

piva / cf / reg. impr. ud
02102200306
rea 235449
info@4youit.net
www.4youit.net

SISTEMA DI GESTIONE QUALITÀ E SICUREZZA INFORMAZIONI

Politica per la qualità e la sicurezza delle informazioni

Informazioni sul documento		
Versione	1.0	
Approvato da	C. Lipone	Direzione
Approvato il	28/04/2025	
Distribuzione	Pubblico	
Doc ID	ISO._000000000003	

Indice

1. Introduzione 3
1.1. Scopo del documento 3
1.2. Perimetro di applicabilità 3
1.3. Destinatari 3
1.4. Reperibilità e divulgazione 3
1.5. Storia del documento 3
2. Politica 4
2.1. Orientamento al cliente 4
2.2. Qualità del servizio e delle tecnologie 4
2.3. Sicurezza delle informazioni 4
2.4. Personale 4
3. Requisiti dei sistemi informatici da rispettare e garantire 4
4. Rischi dei sistemi informatici 5
5. Principi dei concetti di sicurezza dei sistemi informatici 6
6. Misure di sicurezza da adottare 6
7. Obiettivi per la qualità e la sicurezza delle informazioni 6
8. Aggiornamento della politica 6

1. Introduzione

La For You Information Technologies Srl, di seguito "ForYou" o "4You", offre servizi di gestione e controllo dei sistemi informatici e dei loro livelli di sicurezza (MSSP), con attività svolte da persone competenti e professionali.

Nell'ambito delle attività di consulenza e assistenza sistemistica, la 4You, si trova a dover disporre di credenziali di accesso e password riservate fornite dagli stessi clienti allo scopo di eseguire le attività di manutenzione, configurazione e gestione dei propri sistemi informatici. Questo richiede attenzione alla sicurezza da garantire alle informazioni e ai sistemi gestiti.

Senza l'ausilio dei sistemi informatici non è possibile assicurare il raggiungimento degli obiettivi operativi delle aziende a cui la 4You fornisce servizi di assistenza.

Nonostante tutti i vantaggi offerti dalle nuove tecnologie, queste nascondono anche determinati rischi finanziari, etici e legali. Lo scopo di queste direttive è quello di identificare tali rischi, di minimizzarli o escluderli con dovuta considerazione degli aspetti economici.

Il fallimento del sistema informatico di una azienda cliente può comportare considerevoli perdite economiche che possono ripercuotersi negativamente anche sulla 4You sia dal punto di vista economico che da un punto di vista del prestigio aziendale.

Le presenti direttive sulle tecnologie informatiche si propongono di creare ed assicurare le procedure ed i comportamenti necessari per salvaguardare i sistemi informatici dei clienti in assistenza.

1.1. Scopo del documento

Il presente documento stabilisce la politica per la qualità e la sicurezza delle informazioni di 4youit.
Questo regolamento specifica le misure di sicurezza delle informazioni e trattamento dei dati personali di 4youit e sostituisce quello indicato con documento PROC2009_00000002.2.2.

1.2. Perimetro di applicabilità

La presente documento si applica a 4youit.

1.3. Destinatari

Il presente documento è destinato a tutto il personale di 4youit, ai clienti che ne fanno richiesta e ai fornitori critici.

1.4. Reperibilità e divulgazione

La divulgazione e il rispetto di questa procedura sono in carico alla Direzione. Il documento è reperibile sulla intranet aziendale di 4youit.

1.5. Storia del documento

V.	Data	Modifiche effettuate	Approvato da
1.0	28/04/2025	Prima versione	Direzione

2. Politica

2.1. Orientamento al cliente

4You ha come obiettivo la soddisfazione dei clienti e dei loro utenti fornendo un servizio in linea con le innovazioni disponibili per il mercato informatico.

2.2. Qualità del servizio e delle tecnologie

4You ritiene fondamentale garantire la professionalità e l'attenzione del personale e la costante innovazione della proposta tecnologica.
Ai nostri clienti dobbiamo garantire livelli di servizio e di supporto coerenti con le loro aspettative.
4You garantisce rispetto della normativa vigente in materia di qualità e sicurezza delle informazioni.

2.3. Sicurezza delle informazioni

4You ha da sempre condiviso l'obiettivo generale e deontologico della protezione delle informazioni salvaguardandone riservatezza, integrità e disponibilità, con controlli proporzionati al rischio a cui esse sono sottoposte.
I principi cardine a cui attenersi per garantire un adeguato livello di sicurezza per le informazioni trattate sono i seguenti:

- le informazioni sono accessibili solo a coloro che ne hanno necessità (principio need to know);
- il personale è opportunamente formato in materia di sicurezza delle informazioni, privacy e politiche interne;
- i fornitori sono opportunamente controllati secondo quanto applicabile attraverso clausole contrattuali, audit, monitoraggio, condivisione di report e di azioni di miglioramento;
- nei progetti, interni e per i clienti, si considerano i requisiti di sicurezza sin dalla loro ideazione nonché nella progettazione ed erogazione dei servizi;
- ogni opportunità di miglioramento è individuata ed analizzata affinché possa essere colta e permetta a 4You di offrire servizi sempre più adatti ai propri clienti;
- i rischi di sicurezza delle informazioni sono identificati, analizzati, valutati e trattati al fine di prevenirli o ridurne gli impatti, bilanciandoli con il rischio di impresa, la sua sostenibilità e la sua predisposizione all'innovazione;
- i clienti vanno preavvertiti in caso di cambiamenti con impatti significativi;
- la gestione degli incidenti deve essere in linea con quanto stabilito dalla normativa vigente e dalle necessità di raccolta di prove legali.

2.4. Personale

4You è consapevole dell'importanza della crescita professionale e tecnica delle nostre risorse mediante una costante formazione, la condivisione di obiettivi strategici ed il pieno coinvolgimento nella loro realizzazione.
La vocazione alla proattività – cioè la capacità di prevenire ed anticipare i temi ed i bisogni futuri e, più in generale l'abilità nel gestire i cambiamenti – è fondamentale ed è ottenuta come somma di competenze ed esperienze in numerosi settori dell'IT, dei riconoscimenti e delle certificazioni che, insieme al continuo aggiornamento ed autoaggiornamento di conoscenza, tecnologie e logiche applicative, portano alla moltiplicazione delle risorse nel rapporto fiduciario con le aziende clienti.

3. Requisiti dei sistemi informatici da rispettare e garantire

Ai sensi del presente documento, si intende per sistema informatico tutto l'hardware e il software necessari al cliente per il controllo dei rispettivi processi operativi e produttivi, ad esempio: elaborazione ordini, contabilità, fatturazione (o più genericamente "Gestionale"), sistemi di comunicazione email, fax, reti, connessioni internet, server e client.
Finché sussiste un rapporto commerciale con il cliente di natura contrattuale o meno, i requisiti del sistema informatico del cliente che devono essere sempre salvaguardati sono:

1. **Disponibilità**: i servizi, le funzioni o anche l'informazione di un sistema informatico devono poter essere sempre disponibili all'utente-cliente nel momento in cui ne effettua la richiesta; nel rispetto di

questo requisito, ogni attività deve essere concordata con il cliente evidenziando sempre quali possono essere gli impatti sulla disponibilità del sistema informatico. Nei casi in cui si ritiene che questo requisito sia a rischio per le caratteristiche del sistema stesso confrontandolo con le esigenze operative derivanti dall'attività produttiva o commerciale del cliente, si deve documentare per iscritto questo rischio e informare il cliente ed il titolare della 4You.

2. **Integrità:** i dati devono essere completi ed invariati. Devono essere prese le contromisure adatte per impedirne la manipolazione da parte di persone non autorizzate; ogni attività deve essere eseguita nel rispetto di questo requisito ed in caso di necessità è obbligatorio richiedere per iscritto le dovute autorizzazioni dal responsabile che deve essere stato formalmente incaricato dall'organo direttivo del cliente, a svolgere tale funzione;
3. **Riservatezza:** le informazioni ed i dati devono essere considerati sempre ed ovunque come dati "Confidenziali" e devono essere protetti da divulgazione e pubblicazione non autorizzate; nel rispetto di questo requisito è necessario adottare tutte le contromisure necessarie e nel caso dell'invio di dispositivi di memorizzazione ad un centro assistenza, richiedere una autorizzazione per iscritto per l'invio dell'hard disk effettuando o meno tutte le operazioni necessarie per salvaguardare la riservatezza dei dati in esso contenuti;
4. **Autenticazione:** ogni utente che accede a un sistema informatico deve essere soggetto a un processo di autenticazione che controlla l'identità della persona; l'autenticazione deve essere strettamente personale;
5. **Autorizzazione:** il processo di autorizzazione controlla che una persona o un dispositivo siano autorizzati ad eseguire una determinata azione;
6. **Protezione dei dati:** si intende la protezione dei dati del cliente siano essi personali di un utente, siano essi aziendali, contro l'uso improprio da parte di terzi e nel rispetto della legge sulla privacy D.Lgs 196/2003; per garantire questo requisito, ogni tecnico deve conoscere quanto prescritto dalla legge e deve informare tempestivamente il titolare della 4You qualora ritenesse che questo requisito non sia stato rispettato;
7. **Backup dei dati:** il backup dei dati serve per proteggere i dati contro eventuali perdite. A tale scopo devono essere create e gestite delle copie di backup dei dati esistenti sulla base delle specifiche dettate dal cliente o seguendo i requisiti minimi impartiti dalla normativa sulla privacy; nel caso in cui un cliente non disponesse di un adeguato sistema di backup è necessario informare immediatamente il cliente per iscritto e il titolare della 4You.

4. Rischi dei sistemi informatici

L'utilizzo dei sistemi informatici comporta determinati rischi. L'identificazione e la riduzione di tali rischi è la pre-condizione per un impiego responsabile ed economico dei sistemi informatici.

I rischi di sicurezza delle informazioni sono quindi identificati, analizzati, valutati e trattati al fine di prevenirli o ridurne gli impatti, bilanciandoli con il rischio d'impresa, la sua sostenibilità e la sua predisposizione all'innovazione.

I possibili rischi sono:

1. **Guasto dei sistemi informatici:** quando dei singoli sistemi informatici falliscono per problemi tecnici, questo può causare l'arresto parziale o addirittura totale dei processi operativi e produttivi del cliente;
2. **Spionaggio di dati:** Persone non autorizzate ottengono accesso ai dati confidenziali. C'è il rischio di spionaggio industriale e della conseguente perdita del vantaggio sulla concorrenza;
3. **Manipolazione dei sistemi o dei dati:** Modifica non autorizzata dei dati. E' possibile che la manipolazione non venga scoperta o venga rilevata solo con ritardo, creando in questo modo interferenze non corrette al momento della elaborazione dei dati manipolati;
4. **Sabotaggio dei sistemi:** La distruzione intenzionale dei sistemi informatici causa arresti e perdite commerciali;
5. **Perdita di dati:** La cancellazione intenzionale o accidentale di dati per i quali non esistono copie di backup causa arresti e perdite operative.
6. **Pubblicazione di dati riservati:** Danneggia l'immagine dell'azienda e causa perdita di fiducia e rivendicazioni da parte di terzi.

5. Principi dei concetti di sicurezza dei sistemi informatici

Sono necessarie diverse precauzioni che assicurino un utilizzo ottimale dei sistemi informatici al fine di minimizzare i rischi. Si tratta di precauzioni sia organizzative che tecniche. Ogni concetto di sicurezza relativo ad un sistema informatico comprende la descrizione dettagliata delle singole precauzioni. Per ogni cliente/sistema informatico viene redatto un proprio concetto di sicurezza.
Per una positiva attuazione delle presenti direttive è necessario che i concetti di sicurezza informatica rispondano ai seguenti requisiti principali:

1. **Adeguatezza:** deve essere assicurato che il rapporto costi/benefici sia ragionevolmente proporzionato;
2. **Responsabilità chiare:** i concetti devono prevedere l'identificazione del responsabile dell'implementazione delle precauzioni in esso specificate;
3. **Competenza:** è fondamentale garantire la competenza e la professionalità del personale e la costante innovazione della propria proposta tecnologica; il personale va formato anche in materia di sicurezza delle informazioni e privacy e deve seguire la normativa applicabile e le regole e politiche interne
4. **Documentazione:** definizione delle componenti che formano il sistema informatico;
5. **Analisi dei rischi:** descrizione delle possibili perdite o danni risultanti da guasti, funzionamento non corretto, utilizzo improprio, ecc…
6. **Metodi:** in che modo un concetto di sicurezza informatica viene implementato;
7. **Piano di emergenza:** se un sistema informatico fallisce, il piano di emergenza deve assicurare di contenere al minimo i danni e le perdite;
8. **Status:** ciclo di vita di ogni concetto di sicurezza: preparazione -> introduzione -> funzionamento -> controllo -> aggiornamento -> …
9. **Rispetto della normativa:** deve essere garantito il rispetto della normativa vigente in materia di qualità, privacy e sicurezza delle informazioni;
10. **Need-to-know**: le informazioni sono accessibili solo a coloro che ne hanno necessità;
11. **Fornitori:** i fornitori sono opportunamente controllati, secondo quanto applicabile, attraverso clausole contrattuali, audit, monitoraggio, condivisione di report e di azioni di miglioramento;
12. **Sicurezza nei progetti:** nei progetti, interni e per i clienti, si considerano i requisiti di sicurezza sin dalla loro ideazione, nonché nella progettazione dei prodotti e durante tutta l'erogazione dei servizi;
13. **Miglioramento:** ogni opportunità di miglioramento è individuata e analizzata affinché possa essere colta e permetta a 4You di offrire servizi sempre più adatti ai propri clienti.

6. Misure di sicurezza da adottare

Al fine di garantire il rispetto dei requisiti precedentemente indicati e in considerazione dei rischi legati in particolar modo alla sicurezza dei dati, l'intera organizzazione della 4You si fa carico di adottare le misure tecniche e operative descritte nel documento ITP-Misure tecniche operative.

7. Obiettivi per la qualità e la sicurezza delle informazioni

Gli obiettivi sono stabiliti dalla Direzione in occasione di riesami annuali e condivisi con il personale coinvolto nelle attività.
Gli obiettivi sono stabiliti a inizio anno, o in occasione di modifiche maggiori, per ogni processo e sono stabiliti i responsabili.
Ogni obiettivo è specifico, misurabile, raggiungibile, pertinente le nostre attività e il più facilmente monitorabile possibile.
Gli obiettivi sono riesaminati trimestralmente e in occasione del riesame di direzione.

8. Aggiornamento della politica

Questa politica è riesaminata e, se necessario, aggiornata, almeno una volta all'anno in occasione del riesame di direzione annuale o in occasione di modifiche maggiori, al fine di garantirne la continua adeguatezza.