

DOCUMENTO

POLITICHE PER LA SICUREZZA DELLE INFORMAZIONI



Copia controllata n° _____

Copia non controllata data _____

Consegnata a _____

EMISSIONE

Responsabile del Sistema di Gestione

VERIFICA ED APPROVAZIONE

Alta Direzione

REV.	DATA EMISSIONE.	MOTIVO DELL'EMISSIONE / REVISIONE DEL DOCUMENTO
0	31/01/2022	Prima emissione
1	19/09/2023	Aggiornamento contenuti
2	29/05/2024	Aggiornamento contenuti

Indice

1.0 SCOPO E CAMPO DI APPLICAZIONE

2.0 POLITICHE SPECIFICHE DI SICUREZZA DELLE INFORMAZIONI

2.1 Politica per l'utilizzo dei dispositivi portatili

2.2 Politica per il telelavoro

2.3 Politica per il controllo degli accessi

2.4 Politica per l'accesso alle reti e ai servizi di rete

2.5 Politica per la classificazione e il trattamento delle informazioni

2.6 Politica per l'uso e la gestione delle chiavi crittografate

2.7 Politica di schermo e scrivania puliti

2.8 Politica per la sicurezza fisica e ambientale delle informazioni

2.9 Politica dei backup

2.10 Politica per il trasferimento delle informazioni

2.11 Politica per lo sviluppo sicuro di sistemi e processi

2.12 Politica per la gestione delle vulnerabilità tecniche

3.0 RIESAME DELLE POLITICHE PER LA SICUREZZA DELLE INFORMAZIONI

1.0 SCOPO E CAMPO DI APPLICAZIONE

Scopo del presente documento è quello di definire le politiche specifiche del Sistema di Gestione per la Sicurezza delle Informazioni di **Yunique Business**. Il documento si applica a tutti gli aspetti critici di sicurezza delle informazioni che necessitano politiche e controlli.

2.0 POLITICHE SPECIFICHE DI SICUREZZA DELLE INFORMAZIONI

2.1 POLITICA PER L'UTILIZZO DEI DISPOSITIVI PORTATILI

Yunique Business promuove l'utilizzo corretto e in conformità alla legge dei dispositivi portatili di lavoro come PC portatili e telefoni cellulari. A questo proposito l'Azienda si occupa direttamente alla distribuzione dei dispositivi portatili e fornisce linee guida aziendali interne affinché i suddetti dispositivi siano utilizzati correttamente. In particolare, attraverso il regolamento informatico interno e le altre procedure del SGSI, vengono regolati i seguenti temi di fondamentale importanza per salvaguardare le informazioni:

1. La registrazione e l'assegnazione dei dispositivi portatili;
2. I requisiti per la loro protezione fisica;
3. Le limitazioni all'installazione di software;
4. La limitazione della connessione a servizi informatici;
5. I controlli di accesso;
6. La crittografia;
7. La protezione dal malware;
8. I back-up;
9. L'uso di servizi e applicazioni web.

Allo scopo di garantire un corretto utilizzo dei dispositivi portatili, **Yunique Business** effettua formazione, informazione e addestramento continuo in merito, oltre che sulle altre procedure del SGSI.

Tutto ciò è finalizzato al raggiungimento dell'obiettivo principale di sicurezza delle informazioni in termini di riservatezza, integrità e disponibilità delle stesse.

Il responsabile dello sviluppo, il riesame e la valutazione di questa politica e di tutti i controlli associati è il Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni.

2.2 POLITICA PER IL TELELAVORO

Younique Business utilizza frequentemente il lavoro a distanza. Tale casistica verrà trattata all'interno del regolamento addetti al fine di limitare i rischi relativi allo svolgimento di mansioni in telelavoro.

La Direzione si assume comunque la responsabilità di riesaminare la presente politica e i controlli ad essa associati con cadenza almeno annuale.

2.3 POLITICA PER IL CONTROLLO DEGLI ACCESSI

Younique Business ha sede a Capannori (LU) nello stabile appartenente e gestito dalla stessa. Gli accessi e le politiche di accesso sono pertanto gestite da **Younique Business** che ha emesso a tale proposito procedure e linee guida di controllo accessi, così come definito dalle procedure interne, per raggiungere l'obiettivo principale di sicurezza delle informazioni in termini di riservatezza, integrità e disponibilità delle stesse.

Tali procedure prendono in considerazione i seguenti aspetti:

1. Requisiti di sicurezza delle applicazioni di business;
2. Le politiche per l'autorizzazione e la diffusione delle informazioni;
3. La legislazione pertinente ad ogni obbligo contrattuale riguardante la limitazione dell'accesso a dati e servizi;
4. La gestione dei diritti di accesso in un ambiente distribuito e di rete che riconosca ogni tipo di connessione disponibile;
5. Le richieste di accesso, le autorizzazioni di accesso e l'amministrazione dell'accesso;
6. L'aggiornamento periodico degli accessi;
7. La rimozione dei diritti di accesso;
8. I ruoli con accesso privilegiato;
9. L'archiviazione di tutte le registrazioni inerenti il controllo accessi.

I responsabili dello sviluppo, il riesame e la valutazione di questa politica e di tutti i controlli associati sono:

- **Younique Business** per quanto riguarda il controllo accessi in generale;
- di cui il Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni per quanto attiene la gestione dei badge del personale esterno.

2.4 POLITICA PER L'ACCESSO ALLE RETI E AI SERVIZI DI RETE

Yunique Business ha sede a Capannori (LU) nello stabile appartenente e gestito dalla stessa. L'accesso alle reti e ai servizi di rete è gestito in coerenza con la politica di controllo accessi e tramite le proprie procedure interne garantisce:

1. l'identificazione delle reti e dei servizi di rete a cui è possibile accedere;
2. l'identificazione di chi è autorizzato ad accedere alle reti e ai servizi di rete;
3. siano controllati accessi a reti e servizi di rete;
4. l'identificazione di particolari modalità di accesso alle reti e ai servizi di rete (es. VPN) per gestirne in maniera appropriata i controlli;
5. i requisiti per l'autenticazione degli utenti;
6. il monitoraggio dell'uso di reti e servizi di rete.

I responsabili dello sviluppo, il riesame e la valutazione di questa politica e di tutti i controlli associati sono:

- **Yunique Business** per quanto riguarda il controllo accessi in generale;
- di cui il Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni per quanto attiene la gestione dei badge del personale esterno.

2.5 POLITICA PER LA CLASSIFICAZIONE E IL TRATTAMENTO DELLE INFORMAZIONI

Yunique Business al fine di garantire la sicurezza delle informazioni ed in particolare la riservatezza classifica, etichetta e tratta le informazioni in ottemperanza alla procedura **I103 Inventario Asset e Classificazione Informazioni** e in ottemperanza alla legge italiana.

Il responsabile dello sviluppo, il riesame e la valutazione di questa politica e di tutti i controlli associati è il Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni.

2.6 POLITICA PER L'USO E LA GESTIONE DELLE CHIAVI CRITTOGRAFICHE

Yunique Business in caso di necessità indica e rende disponibili, secondo la tipologia di dato o documento, le chiavi crittografiche strettamente necessarie. Nessun lavoratore è autorizzato ad utilizzare controlli crittografici in contrasto col principio sopra enunciato.

Il responsabile dello sviluppo, il riesame e la valutazione di questa politica e di tutti i controlli associati è la Direzione.

2.7 POLITICA DI SCHERMO E SCRIVANIA PULITI

Younique Business crede che la sicurezza delle informazioni parta anche da una corretta pulizia dei luoghi di lavoro, pertanto promuove a tutti i livelli aziendali la pulizia delle scrivanie e il corretto uso delle stampanti per evitare accumulo di informazioni su supporti cartacei che potrebbero essere rubati o modificati. **Younique Business** promuove inoltre la pulizia dei PC e l'utilizzo consapevole degli stessi prevedendo opportune misure per il salvataggio dei file di lavoro. Il responsabile dello sviluppo, il riesame e la valutazione di questa politica e di tutti i controlli associati è la Direzione.

2.8 POLITICA PER LA SICUREZZA FISICA E AMBIENTALE DELLE INFORMAZIONI

Younique Business crede inoltre che la sicurezza delle informazioni parta anche da una corretta pulizia dei luoghi di lavoro, pertanto promuove a tutti i livelli aziendali la pulizia delle scrivanie e il corretto uso delle stampanti per evitare accumulo di informazioni su supporti cartacei che potrebbero essere rubati o modificati. **Younique Business** promuove inoltre la pulizia dei PC e l'utilizzo consapevole degli stessi prevedendo opportune misure per il salvataggio dei file di lavoro. Il responsabile dello sviluppo, il riesame e la valutazione di questa politica e di tutti i controlli associati è la Direzione.

2.9 POLITICA DEI BACKUP

Younique Business, data la peculiarità delle proprie attività, promuove il salvataggio dei dati come aspetto di continuità del business e quindi come fattore strategico per l'Azienda. **Younique Business** mette quindi a disposizione, per le attività che le competono, le risorse necessarie affinché i backup possano essere svolti e verificati con regolarità. A tale proposito vengono assunti i seguenti parametri base:

1. RECOVERY POINT OBJECTIVE: 24 ore;
2. RECOVERY TIME OBJECTIVE: 48 ore.

Resta inteso che i dati sopra citati siano da assumersi in senso generale, rimandando per i casi specifici alle definizioni di specifica presenti nei contratti con i clienti.

Laddove i backup dovessero risultare inefficaci/inefficienti verranno promosse azioni a miglioramento di tali condizioni.

2.10 POLITICA PER IL TRASFERIMENTO DELLE INFORMAZIONI

Youique Business, data la peculiarità delle proprie attività, persegue l'obiettivo di controllare la divulgazione delle informazioni attraverso l'adozione di procedure e controlli che permettano di trasferire dati in sicurezza e garantendone l'integrità, la disponibilità e la riservatezza. Tutti gli operatori sono tenuti a seguire tali regole di comportamento.

Il responsabile dello sviluppo, il riesame e la valutazione di questa politica e di tutti i controlli associati è la Direzione.

2.11 POLITICA PER LO SVILUPPO SICURO DI SISTEMI E PROCESSI

Youique Business garantisce la sicurezza delle informazioni anche durante le fasi di progettazione e sviluppo di sistemi e processi:

1. Definendo i requisiti di sicurezza in fase di progettazione;
2. Definendo i punti di controllo durante la progettazione;
3. Definendo archivi sicuri;
4. Monitorando le capacità degli sviluppatori di evitare, trovare e sanare le vulnerabilità.

Il responsabile dello sviluppo, il riesame e la valutazione di questa politica e di tutti i controlli associati è la Direzione.

2.12 POLITICA PER LA GESTIONE DELLE VULNERABILITA' TECNICHE

Younique Business è organizzata per garantire in modo sistematico che le informazioni sulle vulnerabilità tecniche dei sistemi informativi usati siano ottenute in modo efficiente e tempestivo. In particolare, le esposizioni a tali vulnerabilità vengono valutate e verificate mediante pianificazione di VA dedicati, ed appropriate misure vengono intraprese sulla base delle criticità e dei rischi emersi.

Il responsabile dello sviluppo, il riesame e la valutazione di questa politica e di tutti i controlli associati è la Direzione.

3 RIESAME DELLE POLITICHE PER LA SICUREZZA DELLE INFORMAZIONI

Ogni singolo responsabile deve riesaminare ad intervalli almeno annuali la/e politica/he specifiche che gli sono state affidate. Il riesame deve comprendere una valutazione delle opportunità di miglioramento delle politiche dell'organizzazione e dell'approccio alla gestione della sicurezza delle informazioni in risposta ai cambiamenti dell'ambiente organizzativo, alle condizioni del business, alle clausole legali o all'ambiente tecnico.

I riesami delle politiche specifiche devono tenere conto dei risultati dei riesami della direzione.

Le politiche e i controlli associati riesaminati devono essere riscritti, verificati ed approvati dalla Direzione in accordo alle procedure aziendali.