POLITICA GENERALE DI SICUREZZA DELLE INFORMAZIONI

POLICY AZIENDALE

HkStyleCORP. SRL
Sede
Via Vittorio Veneto, 1207
24030 Presezzo - Bergamo (Italy)
+39 035 45 17 039
italia@hkstyle.tech
team@pec.hkstyle.it

Punto Vendita
Via Gen. Carlo Alberto Dalla Chiesa, 10/8
c/o Centro Le Fontane - 24048 Treviolo - Bergamo (Italy)
+39 035 20 10 08 +39 338 50 02 682
italia@hkstyle.tech
www.hkstyle.tech

C.F/P.IVA: 04116140163 - Reg. Imprese BG-436892 - Codice Univoco Fatt.Elett. M5UXCR1

PRINCIPALI MODIFICHE RISPETTO ALLA VERSIONE PRECEDENTE

REV.	DESCRIZIONE	PREPARATO	VERIFICATO	APPROVATO	DATA
0	EMISSIONE DEFINITIVA	Fabio Alborghetti	Davide Rizzo	Stefano Biffi	01/08/2019
1	REVISIONE	Antonio Marzullo	Stefania Botta	Stefano Biffi	24/04/2024
2	REVISIONE	Antonio Marzullo	Stefania Botta	Stefano Biffi	06/05/2024
3	REVISIONE				
4	REVISIONE				
5	REVISIONE				

HkStyleCORP. SRL
Sede
Via Vittorio Veneto, 1207
24030 Presezzo - Bergamo (Italy)
+39 035 45 17 039
italia@hkstyle.tech
team@pec.hkstyle.it

Punto Vendita
Via Gen. Carlo Alberto Dalla Chiesa, 10/8
c/o Centro Le Fontane - 24048 Treviolo - Bergamo (Italy)
+39 035 20 10 08 +39 338 50 02 682
italia@hkstyle.tech
www.hkstyle.tech

C.F/P.IVA: 04116140163 - Reg. Imprese BG-436892 - Codice Univoco Fatt.Elett. M5UXCR1

INDICE

1. INTRODUZIONE

1.1 SCOPO

Il presente documento raccoglie le principali policy della Sicurezza delle Informazioni applicate in HKStyle.
in termini di principi, linee guida e regole da applicare per la definizione, gestione e governo della sicurezza dei sistemi informativi.
In particolare, questo documento rappresenta lo strumento preferenziale al fine di sensibilizzare i dipendenti e i collaboratori dell'azienda in merito alle norme che devono essere rispettate nella gestione del patrimonio informativo aziendale, con l'obiettivo di garantire la sicurezza del sistema informatico e la tutela dell'immagine

1.2 CAMPO DI APPLICAZIONE

Le politiche di sicurezza definite nel presente documento devono essere applicate per l'intero insieme di strutture organizzative e tecnologiche che costituiscono i sistemi informativi della società.
L'infrastruttura che l'azienda fornisce per i propri servizi sia interni (dipendenti, consulenti) che esterni (clienti, fornitori), è così strutturata:

- *Sistemi di applicazioni*: applicazioni e database che supportano i processi aziendali;
- *Sistemi di elaborazione ed archiviazione*: sistemi che forniscono servizi di elaborazione ed archiviazione delle informazioni,
  quali ad esempio mainframe, sistemi dipartimentali, file server, Storage Area Network, ecc.;
- *Sistemi di infrastruttura*: sistemi che forniscono servizi di rete (ad esempio controller di dominio, Proxy, Mail, DNS, Firewall,
  ecc.);
- *Sistemi di telecomunicazione*: dispositivi che forniscono servizi di telecomunicazione, come ad esempio router e switch,
  nonché apparecchiature di telefonia collegate alla rete dati aziendale (ad esempio, smartphone);
- *Workstation*: postazioni di lavoro fisse e mobili attraverso le quali gli utenti accedono alle risorse informative aziendali;
- *Servizi Cloud*: servizi progettati per fornire un accesso facile e conveniente ad applicazioni e risorse, senza la necessità di infrastrutture o hardware interni. Si specifica che anche le politiche di sicurezza per cui non compare un'esplicita sezione di riferimento al cloud vengono altresì applicate ai servizi Cloud.

2. POLICY

2.1. DOCUMENTAZIONE

L'impostazione dello standard ISO/IEC 27001 è coerente con quella del Sistema di Gestione per la Qualità ISO 9001:2015 ed il Risk management, basandosi su un modello PDCA (plan-do-check-act).

L'obiettivo dello standard è quello di proteggere i dati e le informazioni dalle minacce, al fine di assicurarne l'integrità, la riservatezza e la disponibilità, e fornire i requisiti per adottare un adeguato sistema di gestione della sicurezza delle informazioni.
La norma ISO 27002:2022 è una raccolta di "best practices" che possono essere adottate per soddisfare i requisiti della norma ISO 27001:2022 al fine di proteggere le risorse informative.
Il presente documento è stato definito tenendo anche in considerazione:

- le specifiche e i requisiti definiti nel Regolamento UE 2016/679 – GDPR e successivi provvedimenti emanati dall'Autorità Garante per la protezione dei dati personali;
- le specifiche e i requisiti definiti nello Standard ISO / IEC 27017 chiarendo i ruoli e responsabilità per fornitori di servizi cloud e per i relativi clienti con l'obiettivo di garantire che i dati conservati in cloud siano sicuri e protetti;
- le specifiche e i requisiti definiti nello Standard ISO / IEC 27018 [*Codice di condotta per la protezione delle PII (Personally Identifiable information) nei servizi di public cloud per i cloud provider*] da intendersi come linea guida per i fornitori di servizi cloud pubblici sul miglioramento della gestione dei dati personali al fine di fornire una modalità strutturata, basata sul *privacy by design* dei dati personali in infrastrutture informatiche distribuite (cloud pubblico).

Lo standard ISO/IEC 27017:2022, rientrante tra gli standard ISO/IEC 27001, definisce controlli specifici per fornitori e i clienti dei servizi cloud con la finalità di delineare puntualmente i ruoli e responsabilità dei diversi attori coinvolti per garantire la sicurezza e la protezione dei dati personali conservati in cloud. Tale standard fornisce una guida per servizi cloud in aggiunta a quando disciplinato dalla norma ISO/IEC 27002 focalizzati sui nuovi ulteriori aspetti ossia:

- suddivisione delle responsabilità tra fornitore e clienti dei servizi cloud;
- monitoraggio delle attività del cliente all'interno dell'ambiente cloud;
- allineamento degli ambienti virtuale e cloud;
- attività amministrative e procedure connesse con l'ambiente cloud;
- protezione e separazione degli ambienti virtuali;
- configurazione Virtual Machine;

Lo standard ISO/IEC 27018:2019 definisce una serie di contromisure specifiche fondate sui principi internazionali privacy per la corretta progettazione, sviluppo, attuazione, monitoraggio e misurazione di politiche sulla privacy nei servizi di cloud computing.

2.2. POLITICHE DI SICUREZZA INFORMATICA

La HKstyle ha definito le politiche di sicurezza descritte nel presente documento, in linea con le necessità e gli obiettivi di business, i requisiti di sicurezza e la struttura organizzativa aziendale.
Vengono riportati di seguito i principali obiettivi delle politiche di sicurezza informatica:

- garantire che il patrimonio informativo e informatico sia adeguatamente tutelato rispetto ai rischi di compromissione;
- istituire e mantenere un processo strutturato per l'identificazione e la valutazione del rischio informatico, con lo scopo di applicare gli opportuni controlli e di verificane l'efficacia e l'efficienza nell'ottica del miglioramento continuo e riduzione del livello di rischio identificato;

- assicurare la conformità ai requisiti legali, normativi e contrattuali inerenti alla sicurezza delle informazioni.

Le politiche di sicurezza definite nel presente documento sono state strutturate sulla base delle seguenti aree:

1. Standard internazionale ISO 27001:2022 (descritto al paragrafo 2.1 Documentazione):
   - *Organizzazione della sicurezza*: definizione dei ruoli e delle responsabilità per promuovere comportamenti e controlli al fine di garantire la sicurezza informatica;
   - *Gestione degli asset IT*: criteri tecnici e/o organizzativi per la gestione degli apparati informatici e regole per assegnare un profilo di rischio alle informazioni;
   - *Sicurezza del personale*: regole di comportamento cui il personale deve attenersi;
   - *Sicurezza fisica ed ambientale*: protezione per il personale, per i componenti tecnologici, per i locali e gli archivi cartacei;
   - *Sicurezza operativa e delle telecomunicazioni*: controlli sui processi e sulle attività operative come protezione dei dati trasmessi, e controllo degli accessi ai servizi e sistemi informatici disponibili in rete, tra cui i servizi di cloud computing;
   - *Controllo degli accessi*: controllo degli accessi logici al sistema informativo, secondo precise modalità prestabilite;
   - *Gestione delle chiavi crittografiche:* regole per la gestione delle chiavi crittografiche (creazione, distribuzione, memorizzazione, periodo di utilizzo, backup, dismissione, distruzione, protezione)
   - *Acquisizione, sviluppo e manutenzione dei sistemi*: regole per la gestione, modifica, test e messa in produzione di programmi applicativi, software di base e componenti hardware;
   - *Gestione di eventi e incidenti di sicurezza informatica*: procedure per assicurare la tempestiva gestione e risoluzione di incidenti e malfunzionamenti che possano avere un impatto sulla sicurezza informatica;
   - *Gestione della continuità operativa*: regole per governare il processo di erogazione del servizio anche a fronte di un'interruzione dovuta ad un evento critico;
   - *Conformità a leggi e regolamenti*: criteri e procedure necessarie per gli adempimenti previsti da leggi e regolamenti vigenti;

2. Standard internazionale ISO 27017:2015 e ISO27018:2019 (descritto al paragrafo 2.1 *Documentazione)*
   - *Servizi di Cloud Computing: criteri, processi e attività relativi ai servizi di Cloud Computing come la descrizione della struttura, la definizione di obblighi e diritti del fornitore dei servizi cloud e delle HKstyle.*

2.3. PRINCIPI GENERALI

I principi generali cui HKStyle si ispira nella gestione della sicurezza delle informazioni sono articolati nelle seguenti tematiche:

- Identificazione, classificazione e gestione delle risorse
- Gestione sicura degli accessi logici
- Norme comportamentali per la gestione sicura delle risorse aziendali
- Personale e Sicurezza
- Gestione degli eventi anomali e degli incidenti
- Gestione della sicurezza fisica
- Aspetti contrattuali connessi alla sicurezza delle informazioni
- Gestione della Business Continuity
- Monitoraggio, tracciamento e verifiche tecniche
- Ciclo di vita dei sistemi e dei servizi
- Rispetto della normativa

Di seguito, si riporta, per ciascuna tematica, l'obiettivo e le linee guida definite da HKStyle.

2.4. IDENTIFICAZIONE, CLASSIFICAZIONE E GESTIONE DELLE RISORSE

Obiettivo: garantire la piena conoscenza delle informazioni gestite in HKStyle e la valutazione della loro criticità, al fine di agevolare l'implementazione degli adeguati livelli di protezione.

- Deve esistere ed essere mantenuto aggiornato, nel corso del tempo, un sistema di censimento di tutti i beni materiali ed immateriali da tutelare (informazioni, hardware, software, documentazioni cartacee e supporti di memorizzazione);
- Ogni risorsa (bene materiale/immateriale) deve essere direttamente associabile ad un responsabile.
- Le informazioni devono essere classificate in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza ed integrità coerenti ed appropriati. La criticità delle informazioni deve essere valutata in maniera quanto più oggettiva possibile, attraverso l'utilizzo di adeguate metodologie di lavoro.
- Le modalità di gestione ed i sistemi di protezione per le informazioni e gli asset su cui risiedono devono essere coerenti con il livello di criticità identificato.

I principi generali espressi nel presente paragrafo fanno riferimento ai punti 8 **dell'Allegato A, dello standard UNI CEI ISO/IEC 27001:2022.**

2.5. GESTIONE SICURA DEGLI ACCESSI LOGICI

Obiettivo: garantire l'accesso sicuro alle informazioni, in modo da prevenire trattamenti non autorizzati delle stesse o la loro visione da parte di utenti che non hanno i necessari diritti.

- L'accesso alle informazioni da parte di ogni singolo utente deve essere limitato alle sole informazioni di cui necessita per lo svolgimento dei propri compiti (c.d. principio del "need-to-know"). La comunicazione e trasmissione di informazioni all'interno, così come verso l'esterno, deve fondarsi sullo stesso principio.
- L'accesso alle informazioni, in formato digitale da parte di utenti e sistemi autorizzati, deve essere subordinato al superamento di una procedura di identificazione ed autenticazione degli stessi.

- Le autorizzazioni di accesso alle informazioni devono essere differenziate in base al ruolo ed agli incarichi ricoperti dai singoli individui e devono essere periodicamente sottoposte a revisione.
- E' necessario definire un processo di gestione delle credenziali di autorizzazione e dei relativi profili di accesso.
- I sistemi che costituiscono l'infrastruttura ICT devono essere opportunamente protetti e segregati, in modo da minimizzare la possibilità degli accessi non autorizzati.

I principi generali espressi nel presente paragrafo fanno riferimento in particolare al **punto A.8.5, Allegato A1, dello standard UNI CEI ISO/IEC 27001:2022.**

2.6. NORME COMPORTAMENTALI PER LA GESTIONE SICURA DELLE RISORSE AZIENDALI

- **Obiettivo:** garantire che i dipendenti e collaboratori di HKStyle adottino modelli di comportamento volti a garantire adeguati livelli di sicurezza delle informazioni.
- Gli ambienti di lavoro e le risorse aziendali devono essere utilizzati in modo congruo con le finalità per le quali sono state rese disponibili e garantendo la sicurezza delle informazioni trattate.
- Devono essere definite delle procedure per la gestione ed utilizzo delle informazioni sia su supporto digitale che su supporto cartaceo.
- I sistemi informatici aziendali devono essere impiegati da dipendenti e dai collaboratori secondo procedure approvate.

2.7. PERSONALE E SICUREZZA

Obiettivo: garantire che il personale che opera per conto di HKStyle (dipendenti e collaboratori), abbia piena consapevolezza delle problematiche relative alla sicurezza delle informazioni.

- Nelle fasi di selezione ed inserimento del personale in HKStyle devono essere valutati i livelli di conoscenza degli obiettivi e delle problematiche di sicurezza aziendale in funzione delle attività che dovranno essere svolte.
- Durante la permanenza in HKStyle il personale deve ricevere un'adeguata e continuativa formazione inerente le tematiche di sicurezza dei dati.
- Le modalità di chiusura del rapporto di lavoro con HKStyle dovranno essere coerenti con gli obiettivi di sicurezza aziendale.

I principi generali espressi nel presente paragrafo fanno riferimento **al punto 7,dello standard UNI CEI ISO/IEC 27001:2022.**

2.8. *GESTIONE DEGLI EVENTI ANOMALI E DEGLI INCIDENTI*

Obiettivo: garantire che le anomalie e gli incidenti aventi ripercussioni sul sistema informativo e sui livelli di sicurezza aziendale siano tempestivamente riconosciuti e correttamente gestiti attraverso: sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business.

- Tutti i dipendenti e i collaboratori sono tenuti a rilevare e notificare, a chi di competenza e secondo adeguate procedure, eventuali problematiche legate alla sicurezza delle informazioni.

- Gli incidenti che possono avere un impatto sui livelli di sicurezza devono essere rilevati e gli eventuali danni, potenziali e non, devono essere gestiti, ove possibile, in tempi brevi secondo specifiche procedure.

- Deve esistere un sistema di registrazione e classificazione degli incidenti e degli eventi anomali per effettuare analisi volte al miglioramento dei livelli di sicurezza coerentemente con le reali problematiche riscontrate.

I principi generali espressi nel presente paragrafo fanno riferimento in particolare al **punto A.5.25-27, Allegato A1, dello standard UNI CEI ISO/IEC 27001:2022.**

2.9. *GESTIONE DELLA SICUREZZA FISICA*

Obiettivo: prevenire l'accesso non autorizzato alle sedi ed ai singoli locali aziendali e garantire adeguati livelli di sicurezza alle aree e agli asset mediante i quali vengono gestite le informazioni.

- Deve essere garantita la gestione della sicurezza delle aree e dei locali tramite:
  - l'individuazione delle aree e la classificazione dei locali in base alla criticità delle informazioni elaborate;
  - la definizione dei livelli adeguati di protezione.

- Deve essere garantita la sicurezza delle apparecchiature tramite:
  - la definizione di un'adeguata collocazione delle apparecchiature per l'elaborazione delle informazioni;
  - la messa a disposizione delle risorse necessarie al loro funzionamento;
  - la predisposizione di un adeguato livello di manutenzione.

I principi generali espressi nel presente paragrafo fanno riferimento in particolare **al punto 7 Allegato A1, dello standard UNI CEI ISO/IEC 27001:2022.**

2.10. *ASPETTI CONTRATTUALI CONNESSI ALLA SICUREZZA DELLE INFORMAZIONI*

Obiettivo: assicurare la conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni nei contratti con le terze parti, in accordo con le caratteristiche specifiche della relazione che HKStyle deve instaurare con le terze parti stesse.

- Gli accordi con le terze parti e con gli outsourcer che accedono alle informazioni e/o agli strumenti che le elaborano, devono essere basati su contratti formali contenenti opportuni requisiti di sicurezza.

- Gli accordi con terze parti e con gli outsourcer, ove necessario, devono garantire il rispetto dei requisiti di legge in materia di protezione dei dati personali ("normativa privacy").

I principi generali espressi nel presente paragrafo fanno riferimento in particolare alle principali richieste provenienti dal **Codice in materia di tutela dei dati personali (Reg. UE 2016/679 e s.m.i. GDPR) e al punto A5.19-20 Allegato A1, dello standard UNI CEI ISO/IEC 27001:2022.**

2.11. GESTIONE DELLA BUSINESS CONTINUITY

Obiettivo: garantire la continuità dell'attività di HKStyle e l'eventuale ripristino tempestivo dei servizi erogati colpiti da eventi anomali di una certa gravità, riducendo le conseguenze sia all'interno che all'esterno del contesto aziendale.

- Devono essere attentamente identificati e valutati, in termini di probabilità di accadimento e possibili conseguenze, tutti gli eventi da cui può dipendere un'interruzione della continuità del business.

- Deve essere predisposto un piano di continuità che permetta all'organizzazione di affrontare, in modo organizzato ed efficiente, le conseguenze di un evento imprevisto garantendo il ripristino dei servizi critici in tempi e con modalità che consentano la riduzione delle conseguenze negative sulla missione aziendale.

- Devono essere preparate, validate e opportunamente divulgate tutte le procedure operative ed organizzative necessarie per assicurare l'implementazione del piano di continuità.

- Devono essere periodicamente effettuati i test per tutti i componenti del piano di continuità.

- Deve essere assicurato il mantenimento e l'aggiornamento dei piani e delle procedure di cui ai punti precedenti al fine di garantire l'efficacia del sistema nel tempo a fronte di eventuali cambiamenti organizzativi/tecnologici.

I principi generali espressi nel presente paragrafo fanno riferimento in particolare **al punto 5.29, Allegato A1, dello standard UNI CEI ISO/IEC 27001:2022.**

2.12. MONITORAGGIO, TRACCIAMENTO E VERIFICHE TECNICHE

Obiettivo: garantire la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi al fine di assicurare la sicurezza e la disponibilità dei servizi e delle relative informazioni.

- I sistemi informativi devono essere periodicamente controllati in modo da valutare il corretto funzionamento dei sistemi di sicurezza, hardware e software, implementati, nonché l'eventuale presenza di vulnerabilità non riscontrate o conosciute in passato.

- A fronte dei risultati di tutte le attività di monitoraggio, tracciamento e verifica devono essere effettuate periodiche attività di analisi, volte all'identificazione delle aree critiche e delle opportune azioni correttive e migliorative.
- Devono essere pianificate attività periodiche di audit del sistema di gestione della sicurezza delle informazioni.

I principi generali espressi nel presente paragrafo fanno riferimento in particolare **al punto 8 Allegato A1, dello standard UNI CEI ISO/IEC 27001:2022.**

2.13. CICLO DI VITA DEI SISTEMI E DEI SERVIZI

Obiettivo: assicurare che gli aspetti di sicurezza siano inclusi in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici.

- Nella fase di progettazione e sviluppo devono essere opportunamente considerati gli aspetti di sicurezza. In particolare, devono essere indirizzate le seguenti tematiche:
  - inclusione dei requisiti di sicurezza nelle specifiche funzionali dei servizi e sistemi;
  - adozione di best practice per lo sviluppo e la manutenzione del software;
  - gestione controllata della documentazione;
  - separazione degli ambienti di sviluppo e test con impiego di procedure formali di accettazione nel passaggio fra ambienti.

- Nella fase di esercizio devono essere opportunamente considerati gli aspetti di sicurezza. In particolare, devono essere indirizzate le seguenti tematiche:
  - capacity management dell'infrastruttura tecnologica;
  - securizzazione dei sistemi e dei dati (configuration management, hardening, installazione di sistemi anti-malware, crittografia);
  - utilizzo di procedure di change management;
  - adozione di procedure di backup e restore;
  - adozione di procedure di dismissione controllata dei sistemi (per esempio cancellazione sicura dei dischi);
  - network security: segregazione delle reti, monitoraggio dei gateway (firewall).

- Nella gestione dei servizi devono essere opportunamente considerati gli aspetti di sicurezza. In particolare, devono essere indirizzate le seguenti tematiche:
  - monitoraggio dei sistemi e servizi;
  - gestione utenze;
  - performance monitoring.

I principi generali espressi nel presente paragrafo fanno riferimento in particolare **al punto 8.26, Allegato A1, dello standard UNI CEI ISO/IEC 27001:2022.**

2.14. RISPETTO DELLA NORMATIVA

Obiettivo: garantire il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente la sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni reputazionali.

- Tutti i requisiti normativi e contrattuali in materia di sicurezza del sistema informativo e aventi impatto sul Sistema di Gestione della Sicurezza delle Informazioni devono essere identificati ed analizzati, al fine di valutarne gli impatti sull'organizzazione e sui sistemi informativi.
- I responsabili delle diverse aree devono assicurarsi, ciascuno nell'ambito di propria competenza, che tutte le politiche, le procedure, gli standard e in generale tutta la documentazione relativa alla sicurezza delle informazioni siano applicati e rispettati.
- Il mancato rispetto di quanto indicato in questo documento, e in tutti gli altri che da esso discendono, sarà gestito in ottemperanza a quanto previsto nel CCNL oppure, nel caso di inadempienze di terze parti, secondo i rapporti contrattuali in essere.
- Vengono altresì rispettati tutti i requisiti legali, statutari, regolamentari e contrattuali possono imporre limitazioni alla copia di materiale proprietario. In particolare, possono richiedere che sia utilizzato solo li materiale sviluppato dall'organizzazione o concesso in licenza oppure fornito dallo sviluppatore all'organizzazione (es. diritti di proprietà intellettuale).

I principi generali espressi nel presente paragrafo fanno riferimento in particolare **al punto 5, Allegato A1, dello standard UNI CEI ISO/IEC 27001:2022.**

3. DEFINIZIONE DEI RUOLI E DELLE RESPONSABILITÀ

3.1. STRUTTURA RESPONSABILE DELLA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

La struttura responsabile del sistema di gestione della sicurezza delle informazioni dovrà farsi promotrice, al fine di rendere la politica generale di sicurezza coerente con l'evoluzione del contesto aziendale, delle eventuali azioni da intraprendere a fronte del verificarsi di eventi quali:

- nuove minacce o modifiche a quelle considerate nelle precedenti attività di analisi del rischio;
- significativi incidenti di sicurezza;
- evoluzione del contesto normativo e legislativo in materia di sicurezza delle informazioni;

- risultati di analisi sui costi, impatti, efficacia ed efficienza del sistema di gestione per la sicurezza delle informazioni.

3.2. **RESPONSABILI**

Il Responsabile generale è la persona a cui competono le decisioni di massimo livello riguardo alle tematiche di sicurezza.
In particolare, ha la responsabilità di supportare e garantire l'applicazione delle politiche generali del Sistema di Gestione della Sicurezza delle Informazioni, di definire le politiche idonee di gestione del rischio e di supportare costantemente il processo di sensibilizzazione sulle tematiche di sicurezza.

HkStyleCORP. SRL
Sede
Via Vittorio Veneto, 1207
24030 Presezzo - Bergamo (Italy)
+39 035 45 17 039
italia@hkstyle.tech
team@pec.hkstyle.it

Punto Vendita
Via Gen. Carlo Alberto Dalla Chiesa, 10/8
c/o Centro Le Fontane - 24048 Treviolo - Bergamo (Italy)
+39 035 20 10 08 +39 338 50 02 682
italia@hkstyle.tech
www.hkstyle.tech

C.F/P.IVA: 04116140163 - Reg. Imprese BG-436892 - Codice Univoco Fatt.Elett. M5UXCR1