

1. SCOPO E CAMPO DI APPLICAZIONE

Il presente documento definisce le politiche aziendali specifiche, parti integranti della politica generale del SGI definita dalla Direzione di STARTACROWD S.P.A. SOCIETÀ BENEFIT, relativamente al servizio Cloud, per la protezione dei dati globali, inclusi i dati personali.

Lo scopo di questa politica pertanto è descrivere i principi generali di sicurezza nell'ambito dei servizi in cloud che STARTACROWD S.P.A. SOCIETÀ BENEFIT ha fatto propri, al fine di garantire una sicurezza delle informazioni, conservate e/o gestite su piattaforme in cloud pubblici, di livello almeno pari ai principi generali espressi nella sua politica generale di sicurezza e, in presenza di dati personali, conformi alla normativa vigente.

2. PERIMETRO ORGANIZZATIVO

La presente policy si applica a tutto il personale dipendente di STARTACROWD S.P.A. SOCIETÀ BENEFIT e a tutti i soggetti che collaborano con la stessa.

La policy si applica inoltre a tutti i processi più in generale e a tutte le risorse coinvolte nella gestione delle informazioni trattate dalla società.

Nel documento, i termini "fornitore di servizi cloud" o "CSP", acquistano una duplice valenza a seconda del contesto. Quando la policy verrà applicata a servizi di cui STARTACROWD S.P.A. SOCIETÀ BENEFIT è cliente, con i suddetti termini ci si riferirà al fornitore di tali servizi. Quando verrà applicata a servizi erogati da STARTACROWD S.P.A. SOCIETÀ BENEFIT, ci si riferirà all'azienda.

3. TERMINI E DEFINIZIONI

- **Asset o Bene** – Qualsiasi risorsa che abbia un valore per l'organizzazione, sia essa materiale o immateriale (es. beni fisici, software, informazioni e dati, ...).
- **Cloud** – Un insieme di servizi ICT accessibili on-demand e in modalità self-service tramite tecnologie Internet, basati su risorse condivise, caratterizzati da rapida scalabilità e dalla misurabilità puntuale dei livelli di performance, in modo da poter essere pagati in base al consumo.
- **Cloud Privato** – Piattaforma basata su Cloud gestita internamente per erogare servizi e non aperta alla disponibilità di soggetti terzi.
- **Cloud Pubblico** – Piattaforma basata su Cloud che eroga servizi a più soggetti non connessi tra di loro.
- **Cloud Ibrido** – Soluzione tecnologica che prevede l'impiego combinato di Cloud Pubblico e Cloud Privato.
- **CSP – (Cloud Service Provider)** Un'entità (privata o pubblica) che fornisce piattaforme, infrastrutture, applicazioni, servizi di sicurezza o di archiviazione basati su cloud a un'altra entità/organizzazione solitamente a pagamento.
- **Disponibilità** – Proprietà per la quale le informazioni sono rese accessibili ed utilizzabili su richiesta di un'entità autorizzata (ISO/IEC 13335-1:2004).
- **Hardening** – Insieme di azioni atte ad analizzare le funzionalità di un sistema operativo/applicazione al fine di individuare la configurazione ottima che permetta di innalzare il livello di sicurezza e ridurre il rischio residuo connesso alle debolezze dei sistemi.
- **IaaS – (Infrastructure-as-a-Service)** Infrastruttura erogata in modalità di servizio. Risorse hardware virtualizzate vengono messe a disposizione, affinché l'utilizzatore possa creare e gestire, secondo le proprie esigenze, una propria infrastruttura sul cloud senza preoccuparsi di dove siano allocate le risorse
- **SaaS – Il Software as a Service** è un modello di distribuzione del software basato su cloud in cui il provider di servizi cloud sviluppa e mantiene il software applicativo cloud, fornisce aggiornamenti software automatici e mette il software a disposizione dei propri clienti via Internet basato sul pay-as-you-go.
- **Integrità** – Proprietà per la quale l'accuratezza e la completezza degli asset è salvaguardata (ISO/IEC 13335-1:2004).

- **Log** - Il log è un sistema di registrazione di avvenimenti significativi. I file che contengono queste annotazioni sono detti file di log e potrebbero essere identificati anche come i file delle registrazioni, per cui il log è non è altro che un registro.
- **Responsabile del Trattamento** - la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento; Riservatezza – Proprietà per la quale le informazioni non sono rese disponibili o divulgate a individui, entità o processi non autorizzati (ISO/IEC 13335-1:2004).
- **Snapshot** – Copia dello stato di una macchina virtuale in un determinato momento.
- **Titolare del Trattamento** - la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

4. CONTESTO REGOLATORIO DI RIFERIMENTO

- ISO 27001:2022 – Sistemi di gestione per la sicurezza delle informazioni – Requisiti
- ISO 27002:2023 - Sicurezza delle informazioni, cybersecurity e protezione della privacy - Controlli di sicurezza delle informazioni
- GDPR Reg. UE 679/2016 e legislazione nazionale

5. POLITICA DI SICUREZZA DI GESTIONE SERVIZIO CLOUD

STARTACROWD S.P.A. SOCIETÀ BENEFIT è una PMI innovativa e Società Benefit del settore dell'informazione finanziaria che nasce nel Luglio 2020 con l'obiettivo di migliorare la qualità delle operazioni finanziarie tra imprese e operatori di mercato, fornendo strumenti di analisi avanzati ed informazioni puntuali ed affidabili.

Il servizio in cloud erogato dall'Organizzazione è rappresentato da una piattaforma SaaS di Data Intelligence; per l'erogazione dei servizi in cloud, STARTACROWD S.P.A. SOCIETÀ BENEFIT, fa perno ad una infrastruttura Cloud a supporto dei propri processi, acquisendo il ruolo di Cloud Service Customer.

Il servizio in cloud può essere erogato al Cliente tramite:

- 1) Accesso ad una piattaforma SaaS multi-tenant ospitata su infrastruttura Cloud di STARTACROWD S.P.A. SOCIETÀ BENEFIT, situata presso Google Cloud.

Nell'ambito dell'erogazione e/o gestione di servizi cloud STARTACROWD S.P.A. SOCIETÀ BENEFIT prende in considerazione i requisiti di seguito descritti:

- **Gestione del Cloud:** lo spostamento di dati nel cloud può richiedere un riallineamento significativo di ruoli e responsabilità all'interno dell'organizzazione e/o nei confronti dei suoi fornitori. Per questo motivo è necessario definire puntualmente i ruoli tanto relativamente all'erogazione del servizio quanto alla gestione delle relazioni con i fornitori di servizi cloud.
Il personale con responsabilità dirette relativamente ai servizi su cloud pubblico è formato sulle tecnologie cloud, sulle disposizioni in materia di trattamento di dati personali.
- **Separazione degli ambienti virtuali:** STARTACROWD S.P.A. SOCIETÀ BENEFIT adotta un'architettura multi-tenant con forte isolamento logico tra i dati e gli ambienti di ogni Cliente. Ogni Cliente opera nel proprio ambiente logico, con controllo degli accessi e meccanismi di segregazione dei dati che impediscono l'accesso incrociato tra i dati di diversi Clienti.
- **Gestione delle identità digitali:** la gestione delle identità digitali è una componente essenziale per garantire la sicurezza dei dati nel cloud computing. STARTACROWD S.P.A. SOCIETÀ BENEFIT garantisce una loro corretta gestione durante tutto il ciclo.

- **Gestione dei Log:** STARTACROWD S.P.A. SOCIETÀ BENEFIT dispone delle necessarie informazioni relative ai log di monitoraggio e garantisce l'accesso ai soli utenti autorizzati.
- **Sicurezza delle applicazioni Web:** il cloud è, in genere, un ambiente aperto. Questo aspetto aumenta significativamente l'esposizione agli attacchi. Per questa ragione STARTACROWD S.P.A. SOCIETÀ BENEFIT sottopone a controlli supplementari le applicazioni web che si interfacciano con ambienti Cloud pubblici.
- **Disaster Recovery:** sui dati conservati in Cloud, STARTACROWD S.P.A. SOCIETÀ BENEFIT effettua verifiche puntuali per garantire la loro disponibilità anche in caso di disastro.
- **Indagini informatiche:** In caso di richiesta legale vincolante da parte di autorità governative per la divulgazione dei PII del Cliente, STARTACROWD S.P.A. SOCIETÀ BENEFIT si impegna a notificare tempestivamente il Cliente, a meno che tale notifica non sia proibita dalla legge applicabile.
Per garantire la massima trasparenza e conformità normativa nella gestione della sicurezza, STARTACROWD S.P.A. SOCIETÀ BENEFIT si impegna a definire, documentare e conservare tutte le politiche e le linee guida di sicurezza amministrativa.
- **Trattamento dei dati personali:** i ruoli e le responsabilità nell'ambito del trattamento dei dati personali conservati riportati all'interno del Registro dei Trattamenti dei STARTACROWD S.P.A. SOCIETÀ BENEFIT

Nel seguito vengono descritte le principali attività necessarie per recepire i requisiti sopra riportati.

6. RUOLI E RESPONSABILITÀ PER LA SICUREZZA DELLE INFORMAZIONI

Per consentire un'efficace attività di gestione dei servizi cloud STARTACROWD S.P.A. SOCIETÀ BENEFIT assicura che:

- Il personale con responsabilità dirette relativamente ai servizi su cloud è formato sulle tecnologie cloud, sulle disposizioni in materia di trattamento di dati personali.
- Nel caso di acquisizione di servizi cloud sul mercato, sulla gestione dei fornitori sono definiti e documentati i diversi ruoli e responsabilità per il personale responsabile della gestione del servizio cloud, sono formalizzati Quality Technical agreement per assicurare il livello del servizio erogato, sono inoltre sottoscritti NDA a garanzia della sicurezza e riservatezza delle informazioni.
- Tali ruoli sono condivisi anche con i clienti quando STARTACROWD S.P.A. SOCIETÀ BENEFIT opera in qualità di CSP. Mediante le condizioni specifiche del servizio cloud SaaS sono state identificate le responsabilità del CPS e del Cliente finale.

L'identità del Responsabile del trattamento, è la seguente:

STARTACROWD S.P.A. SOCIETÀ BENEFIT

Sede legale: Via Gino Capponi 24, 50121, Firenze (FI)

Contatti: e-mail info@startacrowd.com

Telefono: +39 334 9197071

Il controllo della gestione in sicurezza dell'infrastruttura Cloud è assicurato da un team di tecnici specialisti composto da risorse interne all'organizzazione STARTACROWD S.P.A. SOCIETÀ BENEFIT e da fornitori esterni qualificati.

Per informazioni di dettaglio:

- Team per la sicurezza – incident@startacrowd.com
- DPO – giulio.vecchi@lcalex.it

7. SEDE GEOGRAFICA TRATTAMENTO DEI DATI

I servizi cloud di STARTACROWD S.P.A. SOCIETÀ BENEFIT sono hostati su Google Cloud Italy S.r.l., dotate dei più alti standard di sicurezza disponibili sul mercato e residenti in server farm geograficamente distribuite nel rispetto delle policy di business del prodotto e delle normative vigenti.

Per informazioni di dettaglio:

- Team per la sicurezza – incident@startacrowd.com

8. GESTIONE DEGLI ASSET E CLASSIFICAZIONE DELLE INFORMAZIONI

L'accesso agli asset informativi dei clienti avviene in relazione alle disposizioni contrattuali ed in conformità con le disposizioni legislative.

A tutela dei diritti degli interessati i cui dati sono oggetto del trattamento, STARTACROWD S.P.A. SOCIETÀ BENEFIT si impegna ad informare i propri clienti sulle politiche, pratiche e tecnologie adottate per la sicurezza delle informazioni e la protezione dei dati personali.

Questi impegni includono:

- Accesso e proprietà dei dati: i clienti mantengono il controllo sui dati e sui contenuti immessi o generati nell'ambito dell'utilizzo della piattaforma. La titolarità dei dati rimane in capo al cliente, fatto salvo per quanto previsto per i dati elaborati e aggregati nell'ambito dei servizi di Data Intelligence;
- Divulgazione dei dati: STARTACROWD S.P.A. SOCIETÀ BENEFIT non divulga i contenuti del cliente se non richiesto dalla legislazione vigente o da ordinanze vincolanti emesse da un'autorità statale. Restano esclusi da tale limitazione i dati e le informazioni oggetto dei servizi di Data Intelligence e Deal Flow management, trattati e resi disponibili secondo le finalità del servizio;
- Controlli di Sicurezza: STARTACROWD S.P.A. SOCIETÀ BENEFIT adotta politiche, standard e linee guida su privacy e protezione dei dati per raggiungere il più alto livello di sicurezza e confidenzialità.

9. GESTIONE ACCESSI UTENTE

Il Servizio SaaS offerto da STARTACROWD S.P.A. SOCIETÀ BENEFIT è una piattaforma di Data Intelligence che supporta la ricerca, l'analisi, la selezione e il monitoraggio di imprese innovative a supporto dei processi di investimento, finanziamento e finanza straordinaria.

Il servizio combina funzionalità avanzate di Data Intelligence a un'infrastruttura collaborativa che consente agli utenti di interagire e condividere informazioni in tempo reale.

All'accesso, l'utente inserisce le credenziali; dopo il login, viene mostrata la homepage della piattaforma, con una dashboard e un menu laterale per navigare tra le varie sezioni disponibili.

Il Cliente è responsabile della gestione degli account dei propri utenti: tramite il pannello di amministrazione può creare, modificare o eliminare utenti, assegnare ruoli e privilegi, e revocare l'accesso in qualsiasi momento.

Alla cessazione del contratto, l'accesso del cliente alla piattaforma viene disabilitato. I dati ed i contenuti riconducibili al Cliente restano disponibili per un periodo stabilito al fine di consentirne l'esportazione, secondo le modalità concordate tra le parti.

Su richiesta del Cliente, o su sollecito di STARTACROWD S.P.A. SOCIETÀ BENEFIT, questi dati possono essere restituiti tramite Dropbox o similare piattaforma di sharing dati, in base al volume dei dati da consegnare. Decorso tale periodo, STARTACROWD S.P.A. SOCIETÀ BENEFIT si riserva di mantenere, cancellare o anonimizzare i dati, in funzione della loro natura e delle finalità del servizio, nel rispetto della normativa applicabile.

10. GESTIONE DELLE CREDENZIALI

La piattaforma assicura una gestione sicura di tutte le credenziali, incluse le password degli utenti.

A tal fine, ci impegniamo a fornire meccanismi tecnici che impongano l'uso di password complesse e uniche, ed a non memorizzare mai le password in chiaro. Le nostre procedure di ripristino delle password sono progettate per garantire che solo gli utenti autorizzati possano recuperare l'accesso ai propri account. Spetta al cliente e al suo personale la responsabilità di mantenere la riservatezza delle credenziali, di non condividerle e di segnalare tempestivamente qualsiasi sospetto di compromissione.

11. VIRTUALIZZAZIONE SUI SISTEMI ACQUISITI SUL MERCATO

La maggior parte dei controlli di separazione logica sulla piattaforma Xeedom non sono fisici. STARTACROWD S.P.A. SOCIETÀ BENEFIT opera per garantire, nell'ambiente virtuale, un livello di sicurezza della separazione dei sistemi almeno analogo a quello degli ambienti fisici, avvalendosi dei servizi gestiti di Google Cloud Platform (region europe-west1) per l'erogazione del servizio Xeedom.

Per consentire un'efficace protezione dei sistemi virtuali, in fase di valutazione del fornitore sono state verificate le politiche di sicurezza adottate, prestando particolare attenzione all'adozione di standard e best practice riconosciuti (ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 1/2/3). Le politiche contemplano i seguenti aspetti:

- esecuzione dei workload applicativi (Xeedom Webapp, Dabacon API) su Google Cloud Run come container serverless gestiti, con esposizione della sola porta applicativa (8080) e disabilitazione di ogni altra interfaccia o servizio non strettamente necessario;
- immagini container costruite a partire da base image minimali (Alpine), sottoposte a build riproducibile e conservate nel registry privato Google Artifact Registry con controlli di accesso IAM;
- configurazione con principi di sicurezza delle informazioni di tutte le interfacce di rete virtuali, dei Virtual Private Cloud (VPC) e delle aree di archiviazione, con connessione al database Cloud SQL tramite Unix socket privato (/cloudsql/) anziché esposizione in rete pubblica;
- limiti sull'utilizzo delle risorse di calcolo e di memoria delle istanze Cloud Run (CPU, RAM, concorrenza, min/max instances, timeout), tali da prevenire esaurimento risorse e garantire l'isolamento tra tenant;
- hardening (adozione di politiche di sicurezza) dei sistemi operativi e delle applicazioni in esecuzione all'interno dei container, patching continuo gestito automaticamente da Google per il runtime Cloud Run sottostante;
- gestione delle chiavi crittografiche e dei segreti applicativi (password database, cron secret, API key) tramite Google Secret Manager, con accesso mediato da Service Account dedicati e policy IAM di tipo least-privilege;
- validazione dell'integrità delle operazioni di gestione delle chiavi tramite audit logging nativo di Google Cloud.

STARTACROWD S.P.A. SOCIETÀ BENEFIT assicura inoltre che i seguenti controlli siano applicati:

- accesso agli access log amministrativi limitato ai soli Service Account e utenti IAM autorizzati, con autenticazione OIDC per l'invocazione dei job da Cloud Scheduler verso Cloud Run;
- registrazione di tutti i log applicativi, di sistema e di audit tramite il servizio nativo Google Cloud Logging, con retention configurata e accesso controllato per ruolo.

STARTACROWD S.P.A. SOCIETÀ BENEFIT identifica l'elenco completo dei suoi fornitori coinvolti nella gestione del cloud per l'erogazione del servizio Xeedom. Il fornitore principale dell'infrastruttura è Google Cloud EMEA Limited (Google Cloud Platform), cui si aggiungono i fornitori elencati nel Registro dei Trattamenti. Nel caso vi siano anche dati personali (PII), STARTACROWD S.P.A. SOCIETÀ BENEFIT assicura l'adempimento di quanto previsto dalla normativa vigente sul trattamento dei dati personali. Il cliente in qualsiasi momento può acquisire informazioni sull'elenco completo dei fornitori coinvolti facendone specifica richiesta via e-mail a privacy@xeedom.ai.

12. SEPARAZIONE DEGLI AMBIENTI

La separazione dei diversi sistemi logici che coesistono su una infrastruttura Cloud è una delle principali misure per garantire la riservatezza e l'integrità dei dati memorizzati oltre che la sicurezza di tutta l'infrastruttura di erogazione del servizio.

STARTACROWD S.P.A. SOCIETÀ BENEFIT implementa una segregazione logica degli ambienti sulla piattaforma Xeedom, assicurando che i dati e le risorse di ciascun cliente siano isolati e non accessibili ad altri clienti. L'isolamento logico è ottenuto tramite separazione a livello applicativo (row-level tenancy sul database relazionale Cloud SQL), policy IAM dedicate sul provider cloud Google Cloud Platform e controlli di accesso granulari sul bucket Cloud Storage utilizzato per i media.

Pur operando talvolta sullo stesso sistema multi-tenant, le funzionalità del servizio impediscono che altri utenti possano inavvertitamente o intenzionalmente visualizzare o modificare i dati di un altro. Questa segregazione logica degli ambienti è un requisito fondamentale per la sicurezza e la conformità normativa, in quanto assicura che il cliente mantenga il controllo totale e la riservatezza dei propri dati sensibili.

Le credenziali e i diritti di accesso sono gestiti in modo sicuro per prevenire conflitti o abusi. Il cliente è responsabile della corretta gestione degli account del proprio personale e della tempestiva revoca degli accessi non più necessari.

Il fornitore esterno di cloud service dovrà fornire a STARTACROWD S.P.A. SOCIETÀ BENEFIT, se richiesto, tutto il supporto necessario a verificare che tale segregazione sia garantita anche quando venissero richiesti elementi di segregazione addizionali nel rispetto delle proprie politiche.

13. GESTIONE DELLE IDENTITÀ DIGITALI

La gestione delle identità digitali è una componente essenziale per garantire la sicurezza dei dati della piattaforma Xeedom. STARTACROWD S.P.A. SOCIETÀ BENEFIT ne garantisce una corretta gestione durante tutto il ciclo di vita dell'identità, in coerenza con quanto previsto nel documento "POL.xx_Politica controllo accessi", cui il presente paragrafo fa rinvio per gli aspetti di dettaglio.

In particolare, sulla piattaforma Xeedom si applicano i seguenti principi:

- provisioning delle credenziali: al primo accesso l'utente riceve credenziali nominative fornite da STARTACROWD S.P.A. SOCIETÀ BENEFIT (username/e-mail e password iniziale) ed è obbligato al cambio password al primo login;
- password policy: il sistema impone l'uso di password complesse (lunghezza minima, combinazione di caratteri alfanumerici e speciali) e non consente la memorizzazione o trasmissione in chiaro; gli hash sono calcolati con algoritmi di derivazione moderni;
- autenticazione a più fattori (MFA): la piattaforma supporta l'attivazione del secondo fattore di autenticazione per aumentare il livello di protezione degli account;
- gestione delle sessioni: le sessioni utente sono gestite dal core applicativo Xeedom con token firmati, scadenza configurata e invalidazione in caso di logout o cambio credenziali;
- controllo degli accessi basato sui ruoli (RBAC): ogni utente è associato a ruoli e permessi che determinano le operazioni consentite; la configurazione dei ruoli è parametrica e gestita da profili amministrativi;
- gestione delegata al Cliente: il Cliente è responsabile della gestione degli account dei propri utenti tramite il pannello di amministrazione e può creare, modificare o disabilitare utenze e revocare gli accessi in qualsiasi momento;
- identità di servizio: l'accesso alle risorse infrastrutturali (Cloud SQL, Cloud Storage, Secret Manager, Cloud Scheduler) avviene esclusivamente tramite Google Cloud Service Account dedicati, con principio del privilegio minimo (least privilege) e separazione dei ruoli;

- ripristino accessi: le procedure di reset password sono progettate per garantire che solo l'utente legittimo possa recuperare l'accesso al proprio account, attraverso token temporanei inviati al canale verificato;
- deprovisioning: alla cessazione del rapporto contrattuale o al venire meno della necessità di accesso, le utenze vengono disabilitate tempestivamente e i relativi privilegi revocati.

14. GESTIONE DEI LOG

STARTACROWD S.P.A. SOCIETÀ BENEFIT dispone delle necessarie informazioni relative ai log di monitoraggio della piattaforma Xeedom e garantisce l'accesso ai soli utenti autorizzati, in coerenza con il modello di controllo accessi descritto al paragrafo precedente.

Il servizio Xeedom, essendo erogato su Google Cloud Platform, fa uso dei servizi nativi di logging e auditing messi a disposizione dal fornitore. In particolare:

- i log applicativi (Xeedom Webapp su Cloud Run, Dabacon API, job schedulati da Cloud Scheduler) sono raccolti in Google Cloud Logging, con retention e policy di accesso configurate secondo le esigenze operative e di compliance;
- i log di attività degli utenti sulla piattaforma (login, azioni rilevanti, modifiche ai dati, richieste di contatto, sblocco informazioni, candidature ad application call) sono registrati sul database core Cloud SQL e disponibili per consultazione da parte dei profili amministrativi autorizzati;
- i log amministrativi e di audit sulle risorse infrastrutturali (Cloud Run, Cloud SQL, Cloud Storage, Secret Manager, IAM) sono raccolti automaticamente da Google Cloud Audit Logs, che tracciano chi ha effettuato quale operazione, quando e da quale identità;
- l'accesso ai log è regolato da policy IAM: solo gli utenti e i Service Account con i ruoli appropriati (ad es. roles/logging.viewer, roles/logging.privateLogViewer) possono consultare i log, secondo il principio del privilegio minimo;
- sono monitorate in particolare tutte le operazioni che richiedono privilegi amministrativi, ivi comprese le operazioni di accesso ai segreti, le modifiche alle policy IAM, i deploy e le operazioni di ripristino dei backup.

Nel caso STARTACROWD S.P.A. SOCIETÀ BENEFIT operi in qualità di CSP, il servizio garantisce ai suoi clienti la possibilità di definire puntualmente i requisiti di monitoraggio, in particolare per quanto riguarda tutte le operazioni che richiedono privilegi amministrativi e le attività rilevanti sul tenant.

15. BACKUP

I dati del Cliente gestiti dalla piattaforma Xeedom sono protetti da un sistema di backup automatico basato sui servizi gestiti di Google Cloud Platform. In particolare, il database relazionale Cloud SQL (MySQL 8.0) su cui risiedono i dati applicativi è configurato con backup automatici giornalieri schedulati nelle ore notturne (fuso Europe/Rome), con storage auto-increase abilitato per evitare interruzioni del servizio dovute a esaurimento spazio. La retention dei backup e l'eventuale abilitazione del Point-in-Time Recovery (PITR) sono gestite secondo le policy interne di STARTACROWD S.P.A. SOCIETÀ BENEFIT e comunque in conformità alle esigenze contrattuali e normative.

I contenuti non relazionali (file caricati dagli utenti, immagini, documenti) sono archiviati su Google Cloud Storage nel bucket dedicato alla piattaforma, con accesso di tipo uniform bucket-level access e con le protezioni native del servizio (ridondanza regionale, durability 99,999999999%).

Le operazioni di ripristino sono effettuate tramite gli strumenti nativi di Google Cloud Platform (snapshot e restore di Cloud SQL, copia / versioning degli oggetti su Cloud Storage), su richiesta e in coerenza con gli SLA definiti con il

Cliente. L'efficacia delle procedure di backup e ripristino viene verificata periodicamente nell'ambito dei test di continuità operativa e disaster recovery di cui al successivo paragrafo.

16. SICUREZZA DELLE APPLICAZIONI WEB

Nel caso di servizi cloud acquisiti sul mercato, STARTACROWD S.P.A. SOCIETÀ BENEFIT ha a disposizione un team (TEAM ISIRT) per gestire gli incidenti di sicurezza e adottare delle linee guida per lo sviluppo delle applicazioni Web che garantisca almeno le misure della PRO.09_Procedura Sviluppo Sicuro e della PRO.05_Procedura di gestione della continuità operativa.

17. DISASTER RECOVERY

I piani di continuità operativa e disaster recovery (BCDR) sono testati annualmente per assicurare la loro efficacia e tempi di recupero (RTO) e punti di recupero (RPO) definiti.

18. INDAGINI INFORMATICHE

Ai clienti dei servizi cloud verrà garantito il massimo supporto, nel rispetto della normativa vigente, nel caso questi avviassero delle indagini sui servizi acquisiti.

Nel caso di servizi cloud acquisiti sul mercato, per consentire un'efficace attività di investigazione, deve essere concordata, con il fornitore qualificato per i servizi cloud, la modalità per la richiesta di dati necessari ad indagini interne ovvero a seguito di richiesta alle autorità legali competenti.

19. REQUISITI CONTRATTUALI

L'adozione dei servizi sul cloud a mercato possono comportare maggiori rischi rispetto all'integrità, riservatezza e disponibilità dei dati. Per questa ragione, i contratti che hanno come oggetto la fornitura di servizi su Cloud Pubblico, devono almeno prevedere:

- Una dichiarazione di "NDA - Non Disclosure Agreement";
- l'espressa dichiarazione che il cliente conserverà il diritto "esclusivo" alla proprietà dei dati per tutta la durata dell'accordo. La proprietà include tutte le copie dei dati disponibili presso il CSP, comprese eventuali copie dei supporti di backup;
- l'espresso divieto per il CSP di utilizzare i dati delle agenzie statali per marketing e/o pubblicità o qualsiasi altro scopo secondario non autorizzato;
- l'indicazione del paese(i) in cui è accettabile che i dati vengano conservati;
- che la normativa sulla protezione dei dati personali applicabile sia conforme alla normativa europea;
- il Service Level Agreement (SLA) del servizio;
- l'obbligo da parte del CSP di informare senza ingiustificato ritardo in merito a qualsiasi violazione dei dati, sia questa confermata o sospetta;
- l'obbligo per il CSP di eliminare completamente qualsiasi traccia di dati/informazioni, al termine dell'Accordo, da tutti i suoi sistemi;
- le modalità con cui il CSP restituirà i dati al termine dell'accordo.

I requisiti di cui sopra andranno rispettati anche nella contrattualizzazione di servizi quando STARTACROWD S.P.A. SOCIETÀ BENEFIT opera in qualità di CSP verso i suoi clienti.

20. PRIVACY E TRATTAMENTO DEI DATI PERSONALI

A tutela dei diritti degli interessati i cui dati sono oggetto del trattamento, il cliente del servizio Cloud, in qualità di Titolare o Responsabile del trattamento, provvede a nominare il CSP, quale Responsabile o Sub- Responsabile del trattamento, con un atto formale.

STARTACROWD S.P.A. SOCIETÀ BENEFIT si impegna a monitorare costantemente lo scenario in continua evoluzione di regolamenti e leggi riguardanti la privacy al fine di identificare i cambiamenti e determinare gli strumenti di cui i clienti potrebbero avere necessità per le esigenze di conformità, in funzione delle loro applicazioni.

STARTACROWD S.P.A. SOCIETÀ BENEFIT si impegna ad informare costantemente i propri clienti su politiche, pratiche e tecnologie di sicurezza dei dati e di privacy applicate.

Questi impegni includono:

- **Accesso e proprietà:** il cliente conserva il pieno controllo dei propri contenuti. La proprietà dei dati rimane al cliente;
- **Divulgazione dei contenuti dei clienti:** STARTACROWD S.P.A. SOCIETÀ BENEFIT non divulgherà i contenuti del cliente se non richiesto dalla legislazione vigente o da ordinanze vincolanti emesse da un'autorità statale;
- **Controlli di Sicurezza:** STARTACROWD S.P.A. SOCIETÀ BENEFIT adotta politiche, standard e linee guida su privacy e protezione dei dati per raggiungere il più alto livello di sicurezza e confidenzialità.

21. MODALITÀ DI AGGIORNAMENTO

Eventuali modifiche ai contenuti del presente documento sono comunicate ai clienti attraverso gli applicativi con accesso ad Internet o al servizio Cloud STARTACROWD S.P.A. SOCIETÀ BENEFIT oppure, segnalate mediante il documento di rilascio alla prima release del software successiva alla modifica di cui in discorso.

La Versione aggiornata del presente documento è comunque sempre consultabile al sito internet www.startacrowd.com in calce alla Home Page.

Edoardo Forconi

Direzione