SECURITY POLICY

ISO 9001

ISO/IEC 27001

ISO/IEC 27017

ISO/IEC 27018

Distribuzione	Destinatari
Controllata	Dipendenti
Non controllata	Stakeholder non dipendenti

Classificazione
☒Pubblico ☐ Ad Uso interno ☐ Confidenziale ☐ Segreto

ED	REV.	DATA	DESCRIZIONE MODIFICA	SCRITTA DA	VERIFICATA DA RESPONSABILE QUALITÀ	APPROVATO DA DIREZIONE
0	0	31/01/2024	Prima emissione	--	RQ	DIR
0	1	25/02/2025	Introdotto modulo reclamo e segnalazioni down time	--	RQ	DIR
0	2	03/02/2026	§2 e §16	CS	RQ	DIR
1	0	30/06/2026	Riadattamento per fusione incorporazione	CS	RQ	DIR

Sommario

1. Backup/Ripristino di emergenza 3
2. Sicurezza dei database 3
3. Sincronizzazione degli orologi 3
4. Sicurezza della password 4
5. Accesso dello staff 4
6. Sicurezza del sistema 4
7. Crittografia dei dati 4
8. Difesa della rete 5
9. Sicurezza del software 5
10. Sicurezza nella progettazione 5
11. Suddivisione delle responsabilità 6
12. Controlli di sicurezza indipendenti 6
13. Compromissione degli account 6
14. Segnalare vulnerabilità di protezione e data breach 7
15. Segnalazione di down-time 7
16. Segnalazioni di reclamo 7

La tua privacy e la tua sicurezza sono importanti per noi. POMIAGER si impegna a gestire i tuoi dati ed a rendere le piattaforme sempre migliori in termini di sicurezza.

1. Scopo

Il presente documento descrive le misure di sicurezza adottate da POMIAGER per proteggere i dati e le informazioni trattati attraverso le proprie piattaforme, nell'ambito del sistema di gestione integrato conforme alle norme ISO 9001, ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018.

2. Campo di applicazione

Il documento si applica a tutte le piattaforme erogate in modalità SaaS da POMIAGER ed è pubblicato su ciascuna di esse. È rivolto a clienti, utenti e altri stakeholder esterni.

3. Backup/Ripristino di emergenza

- Conserviamo i backup completi per ogni database creato sulle nostre piattaforme, con la possibilità di effettuare un restore fino a 30 giorni indietro.
- I backup sono gestiti e conservati tramite servizio cloud.
- Le ubicazioni attuali dei datacenter utilizzati per la storicizzazione dei backup rimangono sempre nella comunità europea (Irlanda Olanda e Italia).
- Puoi contattare l'Helpdesk per ripristinare qualsiasi backup del tuo database attivo.

Ripristino di emergenza:

- RPO (Recovery Point Objective) = da 0 a 24 ore. È la quantità massima di dati che un'azienda può permettersi di perdere durante il processo di recupero, ciò significa che puoi perdere un massimo di 24 ore di lavoro se i dati non possono essere recuperati e se abbiamo bisogno di ripristinare il tuo ultimo backup giornaliero.
- RTO (Recovery Time Objective) = da 0 a 24 ore. In caso di disastro che renda completamente inoperativo uno dei data center, sarà necessario ripristinare il servizio in un altro data center per garantire il recupero dell'operatività.
- I nostri backup giornalieri vengono replicati in diverse posizioni e in vari stati nella comunità europea (Irlanda, Olanda, Italia).

4. Sicurezza dei database

- I dati dei clienti sono archiviati in uno specifico database e non vengono condivisi dati tra i clienti.
- Le regole di controllo per l'accesso ai dati rendono completa la separazione tra i database dei clienti che utilizzano lo stesso cluster. Non è possibile accedere da un database ad un altro.

5. Sincronizzazione degli orologi

- Gli orologi di tutto il sistema di elaborazione delle informazioni pertinenti a POMIAGER o al dominio di sicurezza sono sincronizzati con un'unica fonte di riferimento che girano su Azure Cloud sono generalmente sincronizzati con il servizio di ora (Time service) fornito da Azure. Azure mantiene i suoi orologi dei server sincronizzati con l'UTC (Coordinated Universal Time) attraverso fonti di tempo affidabili come gli orologi atomici e i servizi di tempo via satellite. Questo assicura che tutti i servizi e le macchine virtuali in esecuzione su Azure siano sincronizzati e che l'orario sia coerente in tutta l'infrastruttura cloud. Questo meccanismo di sincronizzazione è fondamentale per molte funzioni

all'interno dell'ambiente cloud, comprese la registrazione degli eventi, la programmazione dei compiti, la gestione delle transazioni e la sicurezza. I clienti di Azure non devono impostare manualmente l'ora nelle loro VM o servizi poiché Azure gestisce automaticamente questa sincronizzazione.

- Il provider NtpClient, che ottiene le informazioni da time.windows.com.
- Il servizio VMICTimeSync, usato per comunicare l'ora dell'host alle macchine virtuali e apportare correzioni dopo che la macchina virtuale viene messa in pausa per la manutenzione.
- Gli host di Azure usano i dispositivi strato 1 di proprietà di Microsoft per mantenere l'ora esatta.

6. Sicurezza della password

- Le password dei clienti sono protette da crittografia standard conforme alle norme del settore PBKDF2+SHA512 (con salt e iterazioni multiple, che rendono più onerosi i tentativi di attacco).
- Lo staff di POMIAGER non ha accesso alla tua password e non può recuperarla per te. Nel caso in cui tu la perda l'unica soluzione è ripristinarla.
- Le credenziali di accesso vengono sempre trasmesse in maniera sicura sugli HTTPS.
- Politiche per le password: gli amministratori dei database hanno un'impostazione integrata per imporre una lunghezza minima della password utente. Altre politiche relative alle password come classi di caratteri richieste non sono supportate per impostazione predefinita perché controproducenti. Vedi ad esempio Shay et al. 2016, e NIST SP 800-63b.
- I nostri applicativi permettono di abilitare la doppia autenticazione (MFA) per rendere ancora più sicura la sicurezza degli accessi.

7. Accesso dello staff

- Lo staff dell'helpdesk delle applicazioni può accedere al tuo account per verificare le impostazioni relative al problema da te segnalato. Per fare ciò, utilizzano le proprie credenziali speciali e non la tua password (delle quali non possono essere in alcun modo a conoscenza).
- L'accesso speciale dello staff migliora l'efficienza e la sicurezza: possiamo riprodurre immediatamente il problema da te segnalato, senza il bisogno di condividere la tua password personale e possiamo verificare e controllare le operazioni dello staff separatamente!
- Lo staff del nostro Helpdesk si impegna al massimo per rispettare la tua privacy ed esegue l'accesso solo ai file e alle impostazioni richieste per diagnosticare e risolvere la tua problematica.

8. Sicurezza del sistema

- Tutti i server cloud degli applicativi eseguono distribuzioni Windows con protezione avanzata con patch di sicurezza aggiornate direttamente dal provider cloud
- Le installazioni sono ad hoc e minime per limitare il numero di servizi che potrebbero contenere delle vulnerabilità.
- Solamente gli amministratori di sistema di POMIAGER hanno l'autorizzazione per gestire da remoto i server.

9. Crittografia dei dati

I dati dei clienti sono sempre trasferiti e archiviati in moduli crittografati (crittografia in transito e a riposo).

- Tutte le comunicazioni di dati alle istanze dei clienti sono protette da crittografia all'avanguardia RSA 2048 bits (SHA256withRSA).
- Tutte le comunicazioni interne di dati tra i nostri server sono protette da crittografia di ultima generazione.
- I nostri server sono sorvegliati in maniera rigidissima per garantirne la sicurezza. Le patch vengono continuamente aggiornate contro le ultime vulnerabilità di SSL. I nostri applicativi beneficiano del **GRADO A** per le valutazioni SSL. Puoi consultarle in ogni momento cliccando su questo link https://www.ssllabs.com/ssltest/index.html
- Tutti i nostri certificati utilizzano moduli solidi di tipo 2048-bit con certificati SHA-2.
- Tutti i dati dei clienti (contenuto dei database e file archiviati) sono crittografati a riposo, sia durante la produzione che nei backup (AES-128 o AES-256)

10. Difesa della rete

- Tutti i fornitori di centri dati utilizzati dagli applicativi Cloud di POMIAGER hanno capacità di rete molto ampie oltre ad un'infrastruttura progettata per sostenere gli attacchi più grandi di tipo OWASP.
- I firewall e i sistemi di prevenzione delle intrusioni sui server aiutano a rilevare e bloccare minacce come attacchi di forza bruta alle password.

11. Sicurezza del software

Gli applicativi di POMIAGER sono sviluppati implementando le best practices per la scrittura di codice sicuro. Vengono svolti attività di formazione interna agli sviluppatori per aggiornarli sulle buone pratiche di sviluppo sicuro. Incoraggiamo gli sviluppatori a verificare i problemi relativi al codice e alla sicurezza. Stiamo sviluppando una pagina sugli applicativi dove vengono riportate informazioni relative alle release e ai bugs conosciuti.

I processi di R&D di POMIAGER constano di steps di revisione del codice che includono gli aspetti relativi alla sicurezza anche per le nuove parti di codice.

12. Sicurezza nella progettazione

I nostri applicativi sono progettati in modo da prevenire l'introduzione delle vulnerabilità di sicurezza più comuni:

- Broken Access Control
- Cryptographic Failures
- Injection
- Insecure Design
- Security Misconfiguration
- Vulnerable and Outdated Components
- Identification and Authentication Failures
- Software and Data Integrity Failures
- Security Logging and Monitoring Failures
- Server-Side Request Forgery (SSRF)

13. Suddivisione delle responsabilità

Sono state definite delle configurazioni standard delle macchine virtuali utilizzate, sono effettuate eventuali personalizzazioni alla configurazione, prendendo a riferimento le linee guida messe a disposizione da agenzie nazionali e internazionali riconosciute, come ad esempio AgID, NIST e il CIS.

POMIAGER eroga le proprie piattaforme in modalità Software as a Service (SaaS). La sicurezza è quindi una responsabilità condivisa tra POMIAGER, in qualità di fornitore del servizio, e il cliente, nei termini di seguito indicati.

Responsabilità del Fornitore (POMIAGER): POMIAGEE è responsabile della sicurezza della piattaforma e dell'infrastruttura su cui è erogata, inclusi: la configurazione e l'hardening dei sistemi, l'installazione delle patch di sicurezza e degli aggiornamenti, il monitoraggio, i backup e il ripristino, la separazione dei dati tra i clienti, la crittografia dei dati in transito e a riposo e la gestione degli accessi del proprio personale. Per l'infrastruttura fisica e di rete fornita dal provider di servizi cloud (Microsoft Azure) valgono le misure da questo adottate.

Responsabilità del Cliente: il cliente è responsabile dell'uso della piattaforma e dei dati che vi inserisce, in particolare: della gestione degli utenti e dei profili di autorizzazione assegnati nella propria istanza; della custodia riservata delle credenziali di accesso, dell'adozione di password robuste e dell'attivazione dell'autenticazione a più fattori (MFA); della sicurezza dei dispositivi e delle reti utilizzati per accedere alla piattaforma; della segnalazione tempestiva di sospette compromissioni degli account, come indicato al §15.

Divisione delle Responsabilità: È essenziale che vi sia una chiara comprensione e documentazione della divisione delle responsabilità tra il fornitore e il cliente in modo da prevenire lacune nella sicurezza e assicurare che entrambe le parti siano consapevoli delle loro rispettive responsabilità. Questa divisione delle responsabilità è dettagliata nei contratti di servizio (SLA) e nelle politiche di sicurezza.

14. Controlli di sicurezza indipendenti

POMIAGER riceve audit da aziende indipendenti che effettuano ispezioni relative alla qualità, alla sicurezza dei dati e delle informazioni e allo sviluppo sicuro dei propri applicativi. Abbiamo implementato un sistema di gestione integrato ISO 9001, ISO/IEC 27001 ISO/IEC 27017 e ISO/IEC 27018.

Effettuiamo test di vulnerabilità e di penetrazione almeno ogni 3 mesi. Il team di sicurezza di POMIAGER riceve i risultati e adotta le misure di correzione idonee se necessario.

15. Compromissione degli account

Qualora avessi percezione di account compromessi (ad esempio sottrazione di credenziali, accessi non autorizzati di terzi) devi segnalare l'evento, senza indebiti ritardi alla mail security@pomiager.com

Faremo delle verifiche di sistema e provvederemo a ripristinare la normale operatività dandotene riscontro.

16. Segnalare vulnerabilità di protezione e data breach

Se hai bisogno di segnalare una vulnerabilità di protezione o un data breach scrivi a privacy@pomiager.com oppure a security@pomiager.com . Le segnalazioni sono trattate con la massima priorità, il problema viene esaminato e risolto dal team sicurezza di POMIAGER, in collaborazione con la persona che ha segnalato il problema per poi essere comunicato adeguatamente agli utenti e ai clienti della relativa piattaforma.

Qualora fosse POMIAGER a rilevare un data breach o un data leak, questo sarà trattato come da procedure interne (PR01MOP_Procedura data breach).

Nei casi in cui il Team di crisi ritenga che la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà degli interessati, il Referente privacy, ha l'obbligo di comunicare la violazione all'interessato, senza ingiustificato ritardo.

17.Segnalazione di down-time

Ci impegniamo a comunicare preventivamente, almeno 72 ore prima, down-time pianificati delle nostre applicazioni, in caso di aggiornamenti di durata maggiore a 1 ora.

18.Segnalazioni di reclamo

Se ritieni necessario segnalare un reclamo, hai diversi strumenti a tua disposizione:

- Puoi chiamare il numero del nostro centralino 0514172555
- puoi scrivere alla mail security@pomiager.com
- oppure puoi utilizzare il tool presente sui nostri siti e piattaforme

Ad ogni reclamo segnalato, POMIAGER si occupa di:

- reagire tempestivamente al reclamo, tenendolo sotto controllo e affrontandone le conseguenze che ne derivano
- reagire a posteriori assicurandosi che non si ripeta altrove.
- tenerti informato sulla gestione

Risponderemo al tuo reclamo e cercheremo di risolverlo entro 5 giorni lavorativi.