## DATI GENERALI

La presente costituisce una Attestazione di Conformità della procedura di Whistleblowing contenuta nel software "Strategic PA" ai requisiti normativi e legislativi di riferimento, in particolare a:

- Legge n. 179/2017 che ha modificato l'articolo 54bis D.Lgs. n. 165/2001
- legge 90/2012 inserendo l'articolo 54bis per la tutela del dipendente pubblico che segnala illeciti nel D.Lgs. 165 del 30 marzo 2001
- Direttiva 2019/1937 riguardante "la protezione delle persone che segnalano violazioni del diritto dell'Unione

Il software per whistleblowing è la soluzione applicativa dedicata alla gestione delle segnalazioni degli illeciti ed è basato sulla piattaforma open source Globaleaks, permettendo di ricevere e gestire in totale sicurezza e in conformità al dettato normativo le segnalazioni ricevute dagli utenti, i quali godono della più assoluta tutela d'identità.

## GARANZIE SULLA PROCEDURA

Di seguito le caratteristiche del software e dell'ambiente di gestione delle segnalazioni.

### Caratteristiche generali del software

- Costantemente aggiornato rispetto agli sviluppi normativi
- Caratterizzato da una infrastruttura applicativa progettata e sviluppata per rispondere efficacemente alle specifiche esigenze in termini di sicurezza e riservatezza, elementi cardine del whistleblowing
- Corretta separazione di dati e procedure per l'inscrizione anagrafica del segnalante e per l'azione di segnalazione
- Configurabilità della struttura informativa dei moduli di iscrizione e di segnalazione;
- Completa configurabilità delle policy di amministrazione
- Possibilità di attivare il canale "anonimo"
- Log di sistema: garantisce la completa tracciabilità delle operazioni svolte sulla piattaforma

### Caratteristiche dell'ambiente di segnalazione

- Garantisce il massimo livello di riservatezza per il segnalante, grazie a specifiche caratteristiche tecniche e funzionali
- Nessuna attività di login utente: l'accesso alle funzionalità di segnalazione avviene mediante inserimento del "codice segnalante" attribuito durante la fase di iscrizione. Il codice segnalante è criptato al pari degli altri dati e conosciuto esclusivamente al segnalante
- Accesso all'interfaccia di monitoraggio della propria segnalazione mediante il "codice segnalazione", attribuito alla fine del processo di segnalazione


**ECOH MEDIA S.r.l.**
**Sede legale e operativa** Via F. Fellini 2, 65010 Spoltore (PE) Tel. 085 9431161 • Fax. 085 9431162
**Sede operativa** Corso Sempione 15/A, 21013 Gallarate (VA) Tel. 0331 259880 • Fax 0331 250059
**Sede operativa** Viale Luca Gaurico 91/93 00143 Roma (RM) Tel. 06 98381868 • Fax 06 98382966
www.ecohmedia.com • info@ecohmedia.com • P. IVA 01448300689 • N° R.E.A. 96954 • Capitale sociale €120.000 i.v.

## Misure di sicurezza

Le seguenti misure di sicurezza della password sono messe in atto al fine di rafforzare la sicurezza del sistema:

- L'Implementazione viene eseguita utilizzando lo strumento zxcvbn che valuta la robustezza della password degli utenti. Una password viene considerata accettabile in base al tempo stimato per il crack, questa è basata sulla presenza di parole comuni, modelli e stima dell'entropia della password che il software calcola
- Modifica della password al primo accesso. Questa funzione costringe il ricevitore a cambiare la propria password al primo accesso. La funzione consente all'amministratore di preparare account di ricevitori mediante una password predefinita o una password scelta dall'amministratore, evitando al tempo stesso utilizzi non sicuri della piattaforma.
- La password viene memorizzata con hashing scrypt casuale a 128 bit, univoco per ogni utente. Il salt viene ottenuto includendo anche il nome utente del destinatario.
- La riservatezza della password trasmessa è fornita da Tor Hidden Services o SSL.
- L'accesso alle segnalazioni è concesso solamente ai destinatari configurati per quel contesto, attraverso un global token generato casualmente ed univoco.
- Se un Receiver ha configurato una chiave di crittografia PGP, i file allegati al Suggerimento verranno crittografati con la loro chiave pubblica.
- Ogni volta che un whistleblower effettua una segnalazione, viene generato un codice numerico segreto a 16 cifre (ricevuta) che permette la visualizzazione successiva della segnalazione. Questo codice non viene direttamente memorizzato nei sistemi ma viene storicizzato solamente l'output di una funzione unidirezionale. La ricevuta della segnalazione agisce come un token di autenticazione per il whistleblower.
- Se la segretezza della ricevuta è compromessa, è possibile accedere al suggerimento con i privilegi di un segnalatore.
- La protezione da attacchi brute force viene applicata sia alla ricevuta del Whistleblower che alla password del ricevente. Se viene rilevata una soglia di oltre 10 tentativi di accesso falliti a livello globale entro 60 secondi, vengono applicate le seguenti misure di sicurezza aggiuntive per rendere meno efficace l'attacco di forza bruta: il sistema inizia a rispondere alle richieste di autenticazione con un ritardo aggiuntivo di 10 secondi; L'obiettivo è quello di rendere inefficiente l'attacco di forza bruta per un utente malintenzionato rallentandolo fino a un punto che rende l'attacco non utile entro un ragionevole lasso di tempo.
- Una volta che un utente si è autenticato, viene generato un ID sessione casuale generato casualmente dal server, lungo 256 bit. Una sessione scadrà di conseguenza a un timeout di inattività dell'utente predefinito:
  - Whistleblower 10 ore
  - Ricevente 10 minuti
- Ogni richiesta effettuata dal client viene protetta da un token XSRF che imposterà l'intestazione http personalizzata "X-XSRFToken".
- È stato implementato un approccio di validazione dell'input basato su whitelist per cui ogni richiesta viene confrontata con un'espressione regolare a cui deve essere conforme. Se non corrisponde, viene generato un errore generico.
- Il ricevente può essere un utente non esperto e potrebbe, inconsapevole, subire un attacco alla sicurezza.
- Per questo motivo un file viene inoltrato ai riceventi solo se supera tutti i controlli di sicurezza configurati: ogni file inviato da Whistleblower viene filtrato per rilevare potenziali rischi associati all'apertura dei file da parte del Destinatario. Se il file caricato è considerato potenzialmente dannoso per i Destinatari viene visualizzato un Disclaimer; I destinatari devono accettare il Disclaimer prima di poter scaricare il file. Viene inoltre visualizzato l'hash dei file caricati consentendo di verificare, tramite scanner virus di terze parti, se il file è un noto malware.


CERTIFICAZIONE DI SISTEMA QUALITÀ DNV·GL ISO 9001

**ECOH MEDIA S.r.l.**
**Sede legale e operativa**
Via F. Fellini 2, 65010 Spoltore (PE)
Tel. 085 9431161 • Fax. 085 9431162

**Sede operativa**
Corso Sempione 15/A, 21013 Gallarate (VA)
Tel. 0331 259880 • Fax 0331 250059

**Sede operativa**
Viale Luca Gaurico 91/93 00143 Roma (RM)
Tel. 06 98381868 • Fax 06 98382966

www.ecohmedia.com • info@ecohmedia.com • P. IVA 01448300689 • N° R.E.A. 96954 • Capitale sociale €120.000 i.v.

- Ogni file caricato viene salvato nel database utilizzando la crittografia AES casuale simmetrica.
- Quando viene effettuata una cancellazione di un file dall'applicazione viene sovrascritto prima di rilasciare lo spazio file sul disco. La routine di sovrascrittura viene eseguita da uno scheduler periodico che agisce nel modo seguente:
  - Una prima sovrascrittura scrive 0 sull'intero file;
  - Una seconda sovrascrittura scrive 1 sull'intero file;
  - Una terza sovrascrittura scrive byte casuali sull'intero file.
- Tutti gli input lato server sono considerati non attendibili e tutti i payload dei messaggi provenienti dai browser degli utenti vengono automaticamente bloccati dal framework dell'applicazione Web.
- Al fine di diagnosticare rapidamente potenziali problemi nel software quando vengono generate eccezioni nei client che vengono inoltrate all'amministratore del server via e-mail.

## Altre funzionalità dichiarate

User Features
- Interamente gestibile da un'interfaccia di amministrazione web
- I whisltleblower possono decidere se e quando dichiarare in modo confidenziale la propria identità
- Scambio file multimediali con whistleblower
- Chat con il whistleblower per discutere la segnalazione
- Personalizzazione del questionario
- Semplice interfaccia del ricevente per la ricezione e l'analisi dei rapporti

Technical Features
- Misurazione automatizzata della qualità del software e test di integrazione continua
- Costruito con tecnologie lightweight framework(AngularJS e Python Twisted)
- Applicazione completamente autonoma (non sono necessari server web o applicazioni)
- Configurazione automatica di Tor Onion Services versione 3
- Supporto HTTP/2

Legal Features
- Questionari pronti per la legge sulla conformità
- Workflow per la segnalazione condizionale dell'identità degli informatori
- Funzionalità di custode per autorizzare l'accesso all'identità del whistleblower
- Criteri di data retension configurabili secondo il GDPR
- Nessun registro di indirizzi IP

Security Features
- Penetration test multipli con report pubblici completi
- Conforme agli standard di settore e alle migliori pratiche per la sicurezza delle applicazioni seguendo le linee guida sulla sicurezza OWASP
- Supporto dell'autenticazione a due fattori (2FA) conforme allo standard TOTP RFC 6238
- Sandbox di rete integrato con iptables
- Sandboxing integrato dell'applicazione con AppArmor


**ECOH MEDIA S.r.l.**
**Sede legale e operativa**
Via F. Fellini 2, 65010 Spoltore (PE)
Tel. 085 9431161 • Fax. 085 9431162
**Sede operativa**
Corso Sempione 15/A, 21013 Gallarate (VA)
Tel. 0331 259880 • Fax 0331 250059
**Sede operativa**
Viale Luca Gaurico 91/93 00143 Roma (RM)
Tel. 06 98381868 • Fax 06 98382966
www.ecohmedia.com • info@ecohmedia.com • P. IVA 01448300689 • N° R.E.A. 96954 • Capitale sociale €120.000 i.v.

- Non lascia tracce nella cache del browser
- Protezione completa contro gli invii automatici (prevenzione dello spam)
- Soggetto a continua peer-review e controlli di sicurezza periodici
- Supporto PGP per notifiche e-mail crittografate

Per approfondimenti vi rimandiamo alla documentazione dell'applicativo (copiare il link):
https://docs.google.com/document/d/1SMSiAry7x5XY9nY8GAejJD75NWg7bp7M1PwXSiwy62U/pub#h.jwnilrzeure5

Quanto sopra indicato viene dichiarato rispondente al vero

**Ecoh Media S.r.l.**
**Amministratore Unico**

**Ecoh Media S.r.l.**
**Responsabile prodotto Strategic PA**