10. Informazioni e Riservatezza

1. Definizioni

Sono riservate tutte le informazioni ritenute di tipo confidenziale, cioè in primo luogo tutte le informazioni tutelate dalla legge, inclusi dati sul personale, salari, informazioni bancarie, informazioni private dei donatori. Inoltre, tutte le informazioni che la direzione dell'organizzazione dichiara essere riservate sono tali, purché la direzione abbia valide ragioni. Ragioni che, ad esempio, hanno a che fare con la privacy di soci e volontari, la loro sicurezza, il rischio legale per l'organizzazione, il successo delle azioni ecc. Greenpeace, in quanto organizzazione della società civile, cercherà ovviamente di essere il più trasparente possibile verso i suoi donatori, sostenitori e verso il pubblico in generale.

2. Informativa di policy dettagliata

2.1 Non divulgherai né diffonderai con alcun mezzo a terzi, informazioni riservate acquisite in virtù della tua posizione, sia in forma verbale che in forma scritta, salvo ove ciò fosse richiesto dalla legge o nel caso in cui tu fossi autorizzato a farlo dall'organizzazione.

2.2 Non utilizzerai le informazioni riservate per ottenere vantaggi per te, per i tuoi parenti o di qualsivoglia terzo.

2.3 Se non sei certo che le informazioni siano da considerarsi riservate o meno, chiedi consiglio al tuo responsabile.

3. Procedure specifiche correlate in materia di prevenzione

Alla Sezione A del documento di premessa, vengono introdotti due approcci alla prevenzione: sensibilizzazione, accesso alle informazioni e formazione del personale ove necessario e risoluzione delle vulnerabilità e dei rischi all'interno di specifici e processi. Questa sezione della policy illustrerà in dettaglio come questi approcci dovranno essere applicati alle violazioni.

Risoluzione di vulnerabilità e rischi
Ciascuna funzione dovrà essere sottoposta ad analisi per determinare in che misura sia vulnerabile agli abusi di informazioni e alle violazioni della riservatezza. I protocolli che intendono ridurre questa vulnerabilità, inclusi ma non in senso limitativo, quelli sopra elencati, dovranno essere esaminati. Una volta analizzati i rischi e le vulnerabilità, sarà possibile adottare adeguate misure per proteggere l'imparzialità di Greenpeace. Protocolli specifici riguardanti proprietà organizzative, servizi e altre risorse:

- Linea di base per la sicurezza delle informazioni
- Valutazione del rischio dei servizi cloud
- Backup
- Protezione dei dati personali
- Misure di controllo della sicurezza del personale
- Misure di controllo della sicurezza fisica
- Misure di controllo della sicurezza tecnica
- Privacy e sicurezza IT
- Utilizzo dei servizi Cloud (software e servizi basati su Internet)

La comunità per l'apprendimento dell'integrità dovrà condividere informazioni su meccanismi di prevenzione efficaci al fine di supportarsi vicendevolmente.

Sensibilizzazione, accesso alle informazioni e formazione
I dipendenti riceveranno adeguata formazione e/o appropriato supporto per quanto riguarda la gestione delle informazioni e la riservatezza, a seconda della loro funzione.

Progetti specifici
Ogni progetto specifico o nuovo dovrà essere valutato per vulnerabilità e rischio, utilizzando la stessa procedura. Possono essere effettuati adattamenti per proteggere le informazioni e la riservatezza di Greenpeace.

4. Monitoraggio e documentazione

Monitoraggio
L'Integrity Officer può scegliere di condurre verifiche periodiche per monitorare se vengono utilizzati i processi e le procedure richiesti.

Documentazione
Oltre alla documentazione delle (sospette) violazioni di questa policy, anche le decisioni prese in merito a progetti speciali dovranno essere documentate per l'apprendimento organizzativo.

Inoltre, i risultati delle analisi dei rischi, di cui sopra, dovranno essere documentati.

5. Come gestire una violazione

Tutte le violazioni di questa policy saranno considerate un problema grave che richiede un'indagine approfondita e, in base alle circostanze, potranno essere intraprese azioni disciplinari. In caso di sospetto di violazione di questa policy, è necessario attenersi al Protocollo di gestione delle (sospette) violazioni.

6. Validità e stato di revisione

Da adattarsi in modo adeguato.