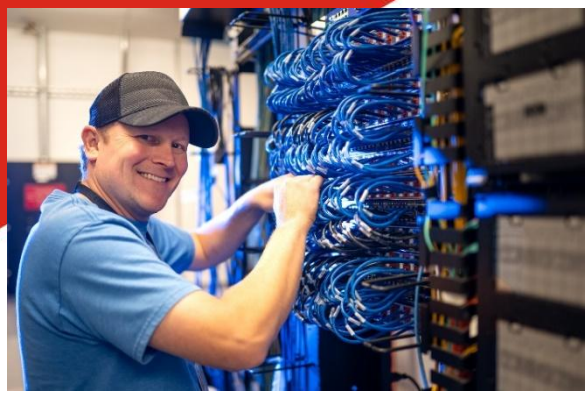
DOC2133

W. L. GORE & ASSOCIATES

UTILIZZO ACCETTABILE

Per i Partner Gore



Introduzione

Gli Hardware o Software (Asset/Risorse Informatiche) di Gore ci offrono la possibilità di stabilire relazioni commerciali con i nostri clienti, i nostri partner e tra di noi. In Gore, crediamo che gli Associati e i Partner agiscano in modo responsabile e dimostrino la dovuta attenzione a proteggere le nostre Risorse Informatiche durante la conduzione dell'attivitá. La presente Policy e il nostro impegno a soddisfare i suoi requisiti sono fondamentali per il nostro successo come azienda.

Obiettivo

Lo scopo della presente Politica di Utilizzo Accettabile ("Policy") è quello di definire le responsabilità dei Partner Gore che accedono o utilizzano gli Hardware o Software ("Asset/Risorse Informatiche") di W. L. Gore & Associates ("Gore"). Questa Policy è stata adottata per proteggere le risorse informatiche di Gore e per guidare i Partner di Gore nell'uso appropriato di tali risorse.

La presente Policy sostituisce qualsiasi Policy di Utilizzo Accetabile precedentemente in vigore. I Partner Gore devono firmare la presente Policy per confermare di aver letto, compreso e accettato di rispettare i contenuti esposti nel presente documento.

Finalità del trattamento

La presente policy si applica a tutti i Partner di Gore che utilizzano gli Asset di Gore.

Tutti gli utilizzi delle risorse informatiche di Gore o l'accesso alle informazioni di Gore, sia su hardware emesso dall'azienda, sia su un dispositivo gestito da Gore di proprietà personale o su un dispositivo non gestito da Gore di proprietà personale (soggetto ad approvazione), sono soggetti a questa politica.

L'omissione da questa Policy non costituisce necessariamente un'autorizzazione. In caso di domande relative ad argomenti non contemplati o a potenziali conflitti, contattare la sua Guida Gore o ITAC.

Definizioni

Le definizioni pertinenti a questa politica sono delineate di seguito. Per ulteriori definizioni, consulti il Glossario IT aziendale.

Strumenti di intelligenza artificiale: qualsiasi applicazione software che utilizza algoritmi di intelligenza artificiale per eseguire attività specifiche e risolvere problemi. Gli strumenti di intelligenza artificiale includono, a titolo esemplificativo:

- *Strumenti di machine learning (ML),* che analizzano i dati per identificare modelli ed effettuare previsioni, aiutando Gore con attività quali la previsione della domanda, la segmentazione dei clienti e il rilevamento delle frodi.
- *Strumenti di elaborazione del linguaggio naturale (NLP, Natural Language Processing),* che elaborano e analizzano il linguaggio umano, consentendo applicazioni come chatbot, analisi del sentiment e l' assistenza clienti automatizzata.
- *Strumenti di visione artificiale (Computer Vision),* che consentono ai computer di interpretare e prendere decisioni basate su dati visivi, utili in aree come il controllo qualità, il riconoscimento facciale e le ispezioni automatizzate.
- *Strumenti di automazione dei processi robotici (RPA, Robotic Process Automation),* che automatizzano le attività ripetitive, come l'immissione dei dati e l'elaborazione delle fatture.
- *Strumenti di analisi predittiva,* che utilizzano algoritmi statistici e tecniche di machine learning per prevedere i

risultati futuri basati su dati storici, aiutando i processi decisionali.
- *IA generativa come LLM (Large Language Model),* che genera contenuti, come testo, immagini o codice, basati su dati di input, che possono essere utilizzati per la creazione di contenuti, il marketing e altro ancora.
- Applicazioni con *RAG (Retrieval Augmented Generation),* che generano contenuti con dati personali, anche se questi dati non provengono dal modello di intelligenza artificiale stesso, ma dall'input, sia esso il prompt dell'Associato o altre fonti di dati consultate.
- *Sistemi di gestione delle traduzioni (TMS, Translation Management System),* che sfruttano l'automazione e possono integrare alcuni elementi di intelligenza artificiale per migliorare il flusso di lavoro della traduzione, come il controllo delle traduzioni precedenti e l'integrazione di nuovi contenuti nel layout del documento originale.

Risorse Informatiche/Asset: qualsiasi hardware o software (emesso da Gore o gestito da Gore) o altro componente dell'ambiente di Gore che supporta le operazioni aziendali e che è di proprietà, concesso in licenza, utilizzato o gestito da Gore.

- L'*hardware* include, a titolo esemplificativo ma non esaustivo, computer, laptop, tablet, dischi rigidi per computer, hardware di rete, unità flash e altri dispositivi di archiviazione, computer, telefoni, dispositivi mobili, apparecchiature per videoconferenze, stampanti, scanner e/o qualsiasi alto apparato tecnologico che supporti le attivitá aziendali.
- Il *software* include, a titolo esemplificativo ma non esaustivo, sistemi operativi, software di rete, applicazioni di messaggistica, come e-mail, segreterie telefoniche, strumenti di messaggistica instantanea e di collaborazione, elaborazione di testi, fogli di calcolo e altre applicazioni dati, database, applicazioni web e/o qualsiasi altro programma, applicazione o piattaforma software.

Contenuti: dati, informazioni o record che hanno valore per l'azienda in base a esigenze operative, legali o normative.

Dati: contenuti che rappresentano una rappresentazione simbolica di qualcosa che dipende, in parte, dai metadati per il loro significato. I dati sono una raccolta di fatti, come numeri, parole, misurazioni, osservazioni o descrizioni di cose.

Responsabile della Protezione dei Dati: il Regolamento generale sulla protezione dei dati (GDPR) ha stabilito il concetto di Responsabile della Protezione dei Dati (DPO, Data Protection Officer) in Europa. Un DPO si impegna a sorvegliare l'osservanza di tutte le leggi in materia di protezione dei dati, monitorare processi specifici e collaborare con le rispettive autorità di vigilanza.

Account e-mail di Gore: account utente (inclusi il software, l'archiviazione e l'hardware) associato a un dominio di Gore che consente di inviare e ricevere e-mail.

Informazioni: contenuti con valore aziendale a breve termine. Le informazioni sono dati nel contesto.

Accesso a Internet: tutte le risorse che consentono la comunicazione elettronica, in particolare il recupero dei dati da Internet, inclusi l'hardware e il software correlati.

Intranet: tutte le risorse fornite da Gore che consentono la comunicazione elettronica sulla rete interna di Gore, inclusi i relativi hardware e software.

Record: contenuti che rappresentano la prova di azioni, decisioni o transazioni aziendali. I record sono informazioni complete e formalizzate in qualsiasi formato (cartaceo o elettronico) che deve essere conservato per periodi di tempo definiti in base a requisiti legali, normativi o operativi.

Dispositivo gestito dall'azienda: dispositivi mobili personali utilizzati per accedere ai contenuti di Gore o alla rete di Gore, su cui è installato e abilitato il software di gestione dei dispositivi Gore.

- Vedere le linee guida per l'uso dei dispositivi mobili

Partner: consulenti, appaltatori, ecc.

Utilizzo delle Risorse Informatiche di Gore

Le attività di Gore devono essere condotte tramite applicazioni approvate o dispositivi gestiti dall'azienda. La mancata osservanza di questo requisito crea il rischio che i contenuti di Gore non siano gestiti in modo appropriato e siano meno sicuri.

È responsabilità di ogni Partner Gore garantire che le Risorse Informatiche i dati e altre informazioni di Gore siano protetti e accessibili unicamente agli utenti autorizzati (Associati e/o Partner).

Accesso

I Partner Gore devono utilizzare solo le Risorse Informatiche a cui gli é stato dato accesso.

I Partner Gore dovranno adottare le seguenti misure quando accedono o concedono l'accesso alle Risorse Informatiche di Gore:

- I Partner di Gore devono accedere o concedere l'accesso alle Risorse Informatiche di Gore utilizzando il principio del "Need to Know".
- I Partner di Gore devono concedere l'accesso alle Risorse Informatiche di Gore solo per il tempo necessario e revocare l'accesso quando i requisiti aziendali sono stati soddisfatti o si verifica un cambio di ruolo.
- Quando necessario, i Partner Gore devono richiedere l'accesso attraverso i canali appropriati (Proprietario dell'applicazione, Sicurezza delle informazioni, ecc.)
- L'accesso remoto alla rete di Gore è consentito solo tramite metodi e dispositivi autorizzati da Gore.

Gestione

I Partner di Gore devono gestire le Risorse Informatiche di Gore in modo sicuro, rispettando le linee guida fornite nella Policy di Classificazione della Sicurezza e nella Policy di Gestione dei Record e delle Informazioni.

Utilizzo non consentito

Ai Partner Gore é fatto divieto di:

- Fare uso illegale o dannoso delle Risorse Informatiche di Gore, in particolare se tale uso puó danneggiare la reputazione di Gore, causare responsabilità o danni finanziari all'Azienda.
- Accedere, scaricare, visualizzare o divulgare materiale che possa essere considerato osceno, razzista, sessista, minatorio, offensivo, discriminatorio o illegale.
- Utilizzare un linguaggio o contenuti minatori, molesti od offensivi.

- Visualizzare contenuti che potrebbero essere ritenuti inappropriati per l'ambiente di lavoro.
- Tentare di eludere qualsiasi misura di sicurezza intrapresa dal team di Sicurezza delle Informazioni (Information Security) o dal team di Sicurezza Fisica di Gore (Physical Security Team).
- Utilizzare le credenziali di accesso di un altro Associato o Partner.
- Connettersi alla rete di Gore utilizzando dispositivi personali non gestiti da Gore.
- Configurare o accedere a qualsiasi rete wireless non autorizzata ad accedere alla rete di Gore.
- Installare o modificare le Risorse Informatiche esistenti o intraprendere un'attività che possa compromettere intenzionalmente o causare un malfunzionamento o un guasto delle Risorse Informatiche di Gore.
- Manomettere o disabilitare il software antivirus o la funzionalità di crittografia di Gore.
- Installare software personale o non standard sulle Risorse Informatiche di Gore (ad eccezione delle app personali su smartphone o tablet).

- memorizzare dati o informazioni di Gore su un dispositivo di proprietà personale (computer, telefono, cloud storage, ecc.), a meno che il dispositivo non disponga di un software di Gore per gestire le informazioni memorizzate su tale dispositivo (vedere l'Accordo per gli utenti di Bring Your Own Device) o in un cloud o in una rete che non sia stata valutata dalla Sicurezza Informatica di Gore.

Monitoraggio

Salvo nei casi vietati dalla legge e al fine di garantire la conformità alle politiche e agli standard aziendali, Gore mantiene il diritto di monitorare, visualizzare, intercettare, bloccare, registrare attività o altrimenti eseguire indagini ("monitorare") qualsiasi utilizzo delle Risorse Informatiche di Gore, da parte di qualsiasi Associato o Partner, e potenzialmente senza preavviso.

Durante il monitoraggio, Gore compierá ogni ragionevole sforzo per rispettare le leggi specifiche del paese al fine di garantire che le informazioni personali ("PI") vengano utilizzate solo per uno scopo specifico e dichiarato.

Quando possibile, il monitoraggio viene eseguito in modo automatico. Durante il monitoraggio, verranno acquisite alcune informazioni. I tipi di informazioni che possono essere raccolti, in determinate circostanze e per scopi specifici, sono riportati nell'Appendice B.

Gore può monitorare, se consentito dalla legge locale vigente, alcune informazioni sensibili (ad es., informazioni soggette a esportazione controllata, informazioni personali o informazioni confidenziali relative la tecnologia Gore ecc.) al fine di rispettare le normative o proteggere la reputazione del marchio Gore e il proprio vantaggio competitivo.

Per quanto riguarda il monitoraggio, possono essere applicate altre procedure regionali o leggi locali. Ulteriori informazioni su come viene eseguito questo monitoraggio per gli Associati sono disponibili nell'Appendice A.

Nella misura consentita dalla legge applicabile, Gore può tentare di identificare un Partner se ha motivo di credere che il Partner Gore stia violando la presente Policy o altre policy correlate. Dopo aver consultato il Responsabile della Protezione dei Dati competente, Gore

puó intraprendere un monitoraggio mirato sul Partner.

Se, attraverso il monitoraggio, Gore sospetta che vi sia stata una violazione della presente Policy:

- si riserva il diritto di rimuovere l' accesso del Partner Gore alle Risorse Informatiche Gore. Laddove necessario, Gore cancellerà o bloccherà l'accesso a qualsiasi informazione aziendale sui dispositivi personali (vedere il contratto Bring Your Own Device).
- Nel rispetto delle leggi vigenti, Gore può archiviare le copie di qualsiasi contenuto acquisito tramite le attività di monitoraggio che riflettono l'uso inappropriato delle Risorse Informatiche di Gore da parte di un Partner Gore. Gore può inoltre divulgare le copie di tali contenuti o di un dispositivo contenente tali contenuti, laddove necessario in caso di contenziosi o indagini.

Dispositivi personali

Gore può consentire ai Partner Gore di utilizzare dispositivi di proprietà personale, come smartphone o tablet, per condurre attività lavorative correlate a Gore. In questi casi:

- I Partner Gore dovranno firmare un Contratto d'uso tramite il processo di richiesta ITAC e consentire a Gore IT di installare il software di Gestione dei Dispositivi Mobili (Mobile Device Management). Il software di gestione dei dispositivi mobili permette a Gore IT di controllare i contenuti e le applicazioni di Gore sul dispositivo, oppure
- Su base limitata, l'accesso può essere concesso secondo il processo di eccezione descritto di seguito.

Comunicazioni elettroniche

Il sistema di posta elettronica di Gore e altri servizi di messaggistica, come Teams o altri strumenti di messaggistica istantanea ("IM") gestiti da Gore e tutte le informazioni contenute all'interno di tali strumenti sono di proprietà esplicita di Gore, salvo se diversamente disposto da disposizioni di legge o normative locali. Gli account e-mail e di messaggistica istantanea (IM) di Gore devono essere utilizzati per lo svolgimento delle attività aziendali. In tutte le comunicazioni elettroniche, è necessario garantire la riservatezza dei dati sensibili e personali (generalmente tramite l'uso della crittografia) in conformità al nostro Standard di Classificazione della Sicurezza.

App di messaggistica

Gore riconosce la necessità di comunicare internamente ed esternamente tramite app di messaggistica istantanea o di comunicazione. Laddove possibile, si consiglia vivamente l'uso di un'app, di una piattaforma o di uno strumento fornito e gestito da Gore e utilizzato su un dispositivo approvato da Gore.

Se è necessario comunicare tramite un'app di messaggistica esterna come WhatsApp, non devono essere trasmesse mai informazioni riservate o sensibili, comprese informazioni personali o di proprietà intellettuale.

I messaggi devono essere principalmente di natura logistica. Non memorizzare mai i dati aziendali di Gore in nessuna app di messaggistica o messaggistica istantanea. Tutti i record aziendali, come le approvazioni e la documentazione di supporto transazionale, devono essere conservati secondo i processi aziendali stabiliti.

Registrazione

I Partner Gore possono utilizzare strumenti (come Microsoft Teams o altre applicazioni) per registrare o trascrivere riunioni e interazioni. I Partner Gore devono informare i partecipanti della registrazione o della trascrizione prima dell'inizio della riunione, preferibilmente nell'invito alla riunione, e consentire ai partecipanti di revocare il consenso se lo desiderano. Se lo strumento di registrazione della riunione non mostra un indicatore chiaro durante la riunione, l'organizzatore deve informare i partecipanti in ritardo che la riunione viene registrata. Per le riunioni ibride e registrate automaticamente, l'organizzatore deve informare tutti i partecipanti della registrazione nell'invito alla riunione o nella chat. Le registrazioni devono essere sospese durante le pause o le discussioni non di lavoro. Le riunioni che coinvolgono argomenti confidenziali o informazioni personali sensibili non devono essere registrate. Alcuni esempi includono: dati dei pazienti, discussioni su contribution o compensation, tecnologia confidenziale di Gore, ecc.

Strumenti di intelligenza artificiale di Gore

I Partner Gore sono incoraggiati a utilizzare gli strumenti di Gore AI **forniti da Gore** per migliorare la produttività, snellire i flussi di lavoro e supportare i processi decisionali. Quando inseriscono dati aziendali o personali negli strumenti di Gore AI, i Partner Gore devono garantire che i dati siano accurati, pertinenti e conformi ai protocolli di privacy e sicurezza dei dati. I Partner Gore non devono caricare o condividere alcun dato negli strumenti di IA non forniti da Gore che sia riservato, sensibile, di proprietá aziendale o protetto da normative, a meno che non sia esplicitamente autorizzato dal leader e valutato dal team di Sicurezza Informatica. Inoltre, i Partner Gore devono essere consapevoli che i risultati generati dall'AI possono talvolta essere fuorvianti o errati. Pertanto, è essenziale verificare l'accuratezza e l'affidabilità dei risultati dell'AI prima di prendere decisioni o intraprendere azioni basate su di essi. I Partner Gore sono responsabili dei risultati generati dagli strumenti di AI e devono essere pronti a spiegare e giustificare tali risultati. L'uso improprio degli strumenti di IA, come la generazione di informazioni fuorvianti, la violazione dei diritti di proprietà intellettuale o l'automazione di compiti senza un'adeguata supervisione, è severamente vietato e può comportare azioni disciplinari, fino al licenziamento.

Conformità e segnalazione

- I Partner Gore dovranno completare qualsiasi formazione associata alla presente Policy, inclusa la formazione obbligatoria sulla Privacy e sulla Sicurezza delle Informazioni.
- I Partner Gore che vengono a conoscenza di qualsiasi incidente di sicurezza che sia effettivo o sospetto o dell'utilizzo o accesso non autorizzato alle Risorse Informatiche di Gore devono informare immediatamente ITAC.
- La violazione della presente Policy, nel rispetto delle leggi vigenti, può dare luogo ad azioni disciplinari, fino alla cessazione del rapporto di lavoro e/o ad azioni legali, ove necessario.

Appendice A - variazioni regionali

Sezione 1	Monitoraggio delle Informazioni per l'Italia	Indica disposizioni aggiuntive rilevanti per gli Associati in Italia.

Sezione 1 - Informazioni di monitoraggio per l'Italia

Le attività di monitoraggio descritte nella presente Policy sono svolte da Gore solo nei limiti e secondo le modalità previste dalla normativa italiana del lavoro e della privacy.

In primo luogo, ai sensi dell'art. 4, par. 1, della Legge del 20 maggio 1970, n. 300, Gore non svolge nessuna di queste attività con lo scopo di monitorare l'attività degli Associati sul luogo di lavoro, ad eccezione di quanto richiesto per ottemperare alle leggi italiane sulla protezione dei dati.

Tuttavia, Gore ha installato strumenti di sicurezza che potrebbero attivare la possibilità indiretta di monitorare le attività degli Associati da remoto.
Tale installazione è necessaria per salvaguardare adeguatamente l'organizzazione e le Risorse Informatiche di Gore.Come identificato in precedenza, identifica e tratta la sicurezza, della fuga di dati sensibili, il rilevamento di frodi, la conformità alle leggi vigenti e l'uso improprio, che creano rischi per l'organizzazione e le Risorse Informatiche di Gore.

Quando possibile, il monitoraggio è condotto su base automatica e/o casuale. Tuttavia, Gore può tentare di identificare un Partner Gore se Gore ha motivo di credere che il Partner abbia commesso una cattiva condotta e tale condotta scorretta possa mettere a rischio l'organizzazione, la sicurezza o le Risorse Informatiche di Gore.

Appendice B - Tipi di informazioni, circostanze e finalità del monitoraggio dell'attività dei Partner Gore sulle Risorse Informatiche Gore.

Sezione 1: Informazioni che possono essere acquisite e registrate durante il monitoraggio

Attività di rete, tra cui:

- Data/ora
- ID utente, ID dispositivo, ID computer, indirizzo IP e altri identificatori univoci
- Percorso fisico e logico dei flussi di dati, tra cui origine e destinazione
- Volume dei dati
- Azioni
- Parole chiave (ad esempio "riservato", "solo per uso interno" ecc.)

Attività su Internet, tra cui:

- Data/ora
- ID utente
- Indirizzo IP di origine
- Indirizzo di destinazione (se consentito)

- Volume dei dati trasferiti

E-mail in entrata e in uscita:

- Data/ora
- Indirizzo del mittente e del destinatario
- ID messaggio
- Dimensione del messaggio
- Oggetto
- Parole chiave relative ai dati sensibili (ad es. "riservato" e "solo per uso interno" ecc.)
- Solo per le e-mail che si attivano per "contenuti segnalati": corpo e allegati delle e-mail.

Gli strumenti di prevenzione della perdita di dati ricercano parole chiave (come "ID paziente") e modelli nei dati per rilevare la potenziale fuga di dati sensibili (come i dati sensibili di clienti, pazienti sanitari o Gore). Questi strumenti monitorano le e-mail in uscita e il traffico in uscita da laptop, desktop e l'utilizzo del cloud (traffico verso web, cloud, USB/CD/DVD, stampanti e unità di rete) e contrassegnano gli elementi specificati.

I dati trattati (che possono contenere identificatori univoci di utente, dispositivo e/o localizzazione) vengono utilizzati solo per i seguenti scopi:

- Analisi e correzione degli errori tecnici.
- Garantire la sicurezza del sistema, inclusa la manutenzione degli elenchi di pagine Internet bloccate ("lista nera").
- Ottimizzazione e controllo degli accessi della rete.
- Controllo della protezione dei dati.

Sezione 2: Esempi specifici di monitoraggio e loro finalitá:

- Protezione delle Risorse Informatiche di Gore da attivitá di divulgazione, eliminazione o alterazione non autorizzate.
- Conformità alle indagini e all'applicazione dei requisiti legali e delle policy Gore.
- Protezione dei sistemi e delle reti da virus, Trojan e altro malware.
- Protezione dei propri sistemi e reti da accessi non autorizzati e/o manipolazioni non autorizzate.
- Protezione dei diritti legali, della sicurezza e protezione di Gore e di altri e
- Come altrimenti richiesto da leggi, regolamenti, ordinanze del tribunale o richieste o requisiti delle autorità competenti o delle forze dell'ordine.