Il Gruppo Fintria ha definito questa Policy Aziendale, quale Regolamento interno, diretta a evitare che comportamenti inconsapevoli possano cagionare danni e favorire rischi per la sicurezza dei dati.

Nella presente Policy di Sicurezza dei dati sono rese note, inoltre, le possibili azioni adottate dal Gruppo Fintria in caso di esigenze organizzative, produttive e di sicurezza del lavoro o in caso di rilevamento di utilizzo anomalo degli strumenti informatici aziendali.

**I dipendenti del Gruppo Fintria, i soci ed i collaboratori interni ed esterni, devono scrupolosamente attenersi alle seguenti istruzioni da considerarsi come ordine di servizio.**

**I dipendenti del Gruppo Fintria, i soci ed i collaboratori interni ed esterni, per esercitare i propri diritti, possono rivolgersi al proprio datore di lavoro.**

## 1. ACCESSO CONSENTITO

a. L'accesso alla sala server ed agli armadi rack di zona è consentito al solo personale autorizzato e munito. Le chiavi per l'accesso ai suddetti locali verrà custodito da persona individuata che terrà anche un registro di ritiro delle chiavi. È fatto divieto di agire su tali apparati se non su espressa indicazione da parte dell'Amministratore di Sistema.

b. L'accesso agli archivi cartacei è consentito solo per effettuare trattamenti dei dati pertinenti alle mansioni di lavoro svolte.

## 2. BANCHE DATI

a. Non si possono eseguire operazioni di trattamento dei dati, per finalità non pertinenti alle mansioni di lavoro svolte.

b. Le banche dati cartacee e informatiche cui si può accedere, devono essere sempre strettamente pertinenti alle mansioni di lavoro svolte e per le finalità previste dall'azienda.

c. L'Amministratore di Sistema assegna a ogni Utente una autorizzazione per l'accesso alla documentazione presente sul Server, per tale motivo non è consentito spostare le cartelle sul server.

d. Si deve operare garantendo la massima attenzione per i dati trattati, dalla loro esatta acquisizione, al loro aggiornamento, così come per la conservazione ed eventuale distruzione.

e. Non devono essere lasciati incustoditi documenti sulla scrivania alla quale possono accedere persone non autorizzate alla visione degli stessi.

f. Negli uffici, al termine delle operazioni di lavoro, gli atti e i documenti cartacei contenenti dati personali, dovranno essere riposti negli archivi di pertinenza e/o dox.

g. Tutti i supporti informatici quali nastri, dischi, cd-rom, chiavette USB, ecc. devono essere resi inutilizzabili, prima di essere eliminati mediante, ad esempio, rottura degli stessi.

## 3. UTILIZZO DELLA STRUMENTAZIONE INFORMATICA E DEI DISPOSITIVI

a. I computer fissi e portatili, i tablet e gli smartphone (Dispositivi Informatici) affidati all'utente sono strumenti di lavoro. Ogni utilizzo non inerente all'attività lavorative può contribuire a innescare disservizi, ma soprattutto minacce per la sicurezza dei dati, pertanto l'utilizzo deve avvenire nel rispetto del vigente Regolamento interno. Tuttavia in caso di necessità personali particolari, di natura occasionale, si potrà chiedere l'autorizzazione all'uso degli strumenti informatici alla Direzione.

b. L'assegnatario è responsabile dei Dispositivi Informatici utilizzati sia durante l'orario di lavoro, sia durante gli spostamenti e oltre l'orario di lavoro se la strumentazione è assegnata in dotazione e/o in comodato d'uso.

c. Non lasciare incustoditi e accessibili i Dispositivi Informatici in dotazione.

d. È vietato modificare il blocco dell'accesso ai PC, che si attiva dopo 15 minuti di inattività.

e. Il PC a fine giornata al fine dell'esecuzione del backup giornaliero va lasciato acceso, l'utente dovrà solamente disconnettersi dall'account. Al termine del backup il PC poi si spegnerà da solo, lasciare un apparecchio incustodito connesso alla rete può essere causa di utilizzo da parte di terzi, senza che vi sia la possibilità di provare in seguito l'indebito uso.

f. È vietata la modifica delle configurazioni dei Dispositivi informatici senza previa autorizzazione dell'Amministratore di Sistema.

g. Avvisare tempestivamente l'Amministratore di Sistema nel caso in cui si riscontrino discrepanze nell'uso degli user-id, modifica e sparizione di dati, cattive prestazioni del sistema, irregolarità nell'andamento del traffico, irregolarità nei tempi di utilizzo del Sistema, difficoltà di connessione, ecc.

h. Non è consentita la visualizzazione, l'utilizzo e il salvataggio sui Dispositivi Informatici aziendali di materiale offensivo, illecito o inappropriato.

i. È vietato caricare sui Dispositivi file di natura personale. L'utente ha però la facoltà di utilizzare immagini e foto personali come sfondo desktop e/o salva video, purché tali immagini non siano di natura volgare e/o offendano il comune senso del pudore, non siano immagini riservate o recanti danno all'azienda; pertanto tali immagini, una volta inserite come fondo desktop o salva video dovranno essere considerati come documenti non riservati. In qualsiasi caso, immagini/foto di persone non devono contenere dati e/o informazioni che possono far riconoscere a terzi l'identità della persona, esempio: foto con nome, foto con numero di telefono, foto e indirizzo di residenza, ecc.

## 4. STAMPANTE DI RETE

a. È cura dell'Utente effettuare la stampa dei dati e documenti solo se strettamente necessaria e di ritirarla prontamente dalla stampante di rete.

## 5. GESTIONE E ASSEGNAZIONE DELLE CREDENZIALI DI AUTENTICAZIONE

a. Le credenziali di autenticazione per l'accesso ai Dispositivi utilizzati per l'attività lavorativa sono assegnate dall'Amministratore di Sistema.

b. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'Utente (User ID), associato a una password.

c. Modificare al primo utilizzo, la password della configurazione di partenza assegnata dall'Amministratore di Sistema.

d. Creare una nuova password associata al codice identificativo (User ID).

e. L'insieme di caratteri alfanumerici che compongono la password devono essere scelti in modo che essa sia difficilmente ricostruibile.

f. La password deve essere cambiata almeno ogni 3 mesi.

g. Le password non devono essere condivise con nessuno, inclusi i colleghi e famigliari.

h. Accedere ai Dispositivi utilizzando esclusivamente le proprie credenziali.

i. Adottare particolari cure e cautele al fine di evitare, l'acquisizione indebita da parte di terzi delle credenziali di accesso.

j. La password deve essere memorizzata e non annottata su documenti personali facilmente identificabili, come agende o rubriche o stickers incollati sulle apparecchiature.

k. Nell'eventualità di dimenticanza della password in uso, l'Utente dovrà chiedere all'Amministratore di Sistema il rilascio di una nuova password. Sarà cura dell'Utente utilizzare tale password per il primo accesso e provvedere all'immediata sostituzione con una di sua sola conoscenza.

l. Relativamente alla gestione delle credenziali di autenticazione l'Amministratore di Sistema:
   I) Non può assegnare il Codice per l'identificazione, laddove utilizzato, ad altri incaricati, neppure in tempi diversi
   II) Deve disattivare le credenziali di autenticazione non utilizzate da almeno sei mesi
   III) Deve disattivare le credenziali di autenticazione, in caso di perdita della qualità che consente all'Utente l'accesso agli strumenti informatici
   IV) Almeno annualmente deve verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione

## 6. INSTALLAZIONE E UTILIZZO DI PROGRAMMI

a. Non è consentito installare autonomamente sul proprio PC programmi provenienti dall'esterno, o installare dispositivi di memorizzazione, comunicazione o altro o utilizzare programmi diversi da quelli distribuiti e installati dall'Amministratore di Sistema, salvo previa autorizzazione esplicita dell'Amministratore di Sistema o della Direzione.
b. L'inosservanza di questa disposizione, infatti, oltre al rischio di portare virus informatici e di alterare la stabilità delle applicazioni per incompatibilità con software esistenti, può esporre l'Azienda a gravi responsabilità civili e anche penali in caso di violazione della normativa a tutela dei diritti di autore sul software, che impone la presenza nel sistema di solo software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.
c. È vietato cancellare, disinstallare, copiare o asportare deliberatamente programmi software.

## 7. UTILIZZO E CONSERVAZIONE DEI SUPPORTI RIMOVIBILI

a. Tutti i supporti magnetici rimovibili (cd e dvd riscrivibili, supporti USB, ecc.) contenenti dati personali e informazioni costituenti know-how aziendale, devono essere utilizzati e custoditi con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

## 8. PROTEZIONE ANTIVIRUS

a. Ogni utilizzatore di Dispositivi Informatici deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale da virus o altro software aggressivo.
b. Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il dispositivo e segnalare prontamente l'accaduto all'Amministratore di Sistema.
c. Ogni dispositivo magnetico di provenienza esterna alla Step Impianti Srl dovrà essere verificato mediante programma antivirus prima dell'utilizzo e nel caso venga rilevato un virus, dovrà essere consegnato all'Amministratore di Sistema.

## 9. BACK UP DEI DATI

a. Affinché vengano garantiti i salvataggi dei dati sul server e in copia mediante back-up, è necessario e obbligatorio che i file vengano salvati sui dischi dei server e non sul desk top del PC.

b. Tutti i dati residenti sul Server aziendale sono salvati quotidianamente su dispositivi di back-up, come previsto dalle procedure di sistema. È fatto obbligo agli utilizzatori dei PC, alla fine dell'orario di lavoro di spegnere i PC e il relativo gruppo di continuità, in modo da garantirsi che i file possano essere copiati. Casi particolari di necessità di lasciare accesi i PC oltre il normale orario di lavoro, devono essere concordati con la Direzione.

c. L'Amministratore di Sistema verifica il ricevimento del report automatico di backup tramite mail.

## 10. INTERNET

a. La navigazione sulla rete internet, è consentita solo per finalità pertinenti alle mansioni di lavoro svolte. Pertanto non è consentito l'utilizzo di internet per scopi personali come ad esempio per l'utilizzo delle web-mail; per scaricare, ascoltare e vedere file musicali e video; effettuare ogni genere di transazioni finanziarie; registrazione a siti; partecipare a forum, chat, social media.

b. È fatto assoluto divieto di navigare su siti pedopornografici, pornografici e similari.

c. Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, Step Impianti Srl potrebbe adottare sistemi di blocco o filtro automatico che, ad esempio, prevengano determinate operazioni quali l'upload o l'accesso a siti in black list.

d. In caso che per motivi di lavoro si renda necessario scaricare dalla rete internet grandi quantità di dati (maggiori di 5 MB) è preferibile eseguire tale operazione durante le ore dove l'attività di ufficio non è a regime cioè, mattina presto, ora di pausa pranzo e sera; in modo che si riduca il rischio che altri eventuali utenti siano in rete e riducano le loro prestazioni di navigazione.

## 11. POSTA ELETTRONICA

a. La casella di posta elettronica assegnata all'utente, anche se nominativa, è uno strumento di lavoro. Non è consentito utilizzarla per finalità non pertinenti alle mansioni di lavoro svolte.

b. È fatto divieto di utilizzare le caselle di posta elettronica assegnata per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione della Direzione.

c. Non è consentito creare aspettative di confidenzialità personale nei destinatari dei messaggi di posta elettronica, in quanto le risposte potrebbero essere conosciute all'interno dell'Azienda. A tale motivo i messaggi di posta elettronica, dovranno avere, oltre al logo aziendale, anche l'avviso per la Privacy.

d. Il sistema di posta elettronica consente, in caso di assenze programmate, d'inviare automaticamente messaggi di risposta predefiniti che possono contenere i riferimenti di un collega a cui rivolgersi per la durata dell'assenza.

e. Si può consentire altresì al dipendente, in caso di assenza improvvisa o prolungata, di inoltrare automaticamente i messaggi di posta indirizzati a sé o all'ufficio, a un collega che a sua volta inoltrerà al responsabile quelli ritenuti urgenti per l'attività lavorativa.

f. Tutta la posta elettronica è considerata posta aziendale e, come ogni file salvato nei server aziendali, viene mantenuta copia di back-up necessaria ai fini del lavoro e conservata per 5 anni.

g. Al cessare del rapporto di lavoro viene attivata la procedura di disattivazione dell'account di posta elettronica. Sarà inoltre creato un messaggio di risposta automatico per avvisare che la casella di posta non è più attiva, che il soggetto fisico individuato quale destinatario non leggerà le comunicazioni e il nuovo indirizzo di posta elettronica a cui far riferimento.

h. È necessario porre la massima attenzione nello scaricare e aprire file allegati ai messaggi di posta elettronica. È vietato eseguire download di file eseguibili o documenti da siti Web o FTP non conosciuti o altre fonti non sicure.

## 12. GESTIONE E MANUTENZIONE DEI DISPOSITIVI INFORMATICI

a. Gli accessi ai Dispositivi Informatici possono essere effettuati, dall'Amministratore di Sistema o da personale autorizzato, per motivi tecnici e/o manutentivi (ad esempio aggiornamenti/sostituzioni/implementazione di programmi software, manutenzione hardware) ai fini di garantire la funzionalità e la sicurezza del sistema informatico.

b. L'Amministratore di Sistema o il personale autorizzato, ha la facoltà di collegarsi e visualizzare in remoto il desktop dei computer ed effettuare ogni tipo di collegamento ai Dispositivi, al fine di garantire l'assistenza tecnica e la normale attività operativa, nonché la massima sicurezza contro virus, spyware, malware, ect. L'intervento viene effettuato su chiamata dell'utente o , in caso di oggettiva necessità, dall'Azienda a seguito della rilevazione tecnica di problemi sul sistema informatico.

c. Detto intervento potrà comportare l'accesso ai dati trattati dagli utenti, ivi compresi gli archivi di posta elettronica e siti internet visitati dagli utenti, sempre nel rispetto di quanto previsto dalla legge di volta in volta in vigore e nel rispetto del presente Regolamento Interno e delle finalità indicate nello stesso. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Azienda, si applica anche in caso di assenza prolungata o impedimento dell'Utente.

d. Il riscontro di un utilizzo indebito dei Dispositivi Informatici o della mancata applicazione degli ordini di servizio riportati nella presente Policy di Sicurezza dei dati genera un avviso di ordine generale e non personale. Successivamente, solo al persistere del problema, saranno generati avviso e provvedimenti direttamente alle persone afferenti.

## 13. CONTROLLI DI SICUREZZA DELL'AZIENDA

a. Nei casi in cui si ritenga indispensabile e/o indifferibile accedere ai Dispositivi Informatici in dotazione a dipendenti, soci e collaboratori interni o esterni per esigenze dirette a garantire la sicurezza e la salvaguardia dei dati e del sistema stesso, si informa che l'accesso agli stessi Dispositivi Informatici, potrà essere effettuato mediante intervento dell'Amministratore di Sistema .

b. Detto intervento potrà comportare l'accesso ai dati trattati dagli utenti, ivi compresi gli archivi di posta elettronica e siti internet visitati dagli utenti, sempre nel rispetto di quanto previsto dalla legge di volta in volta in vigore e nel rispetto del presente Regolamento Interno e delle finalità indicate nello stesso. La

stessa facoltà, sempre ai fini della sicurezza del sistema, si applica anche in caso di assenza prolungata o impedimento dell'Utente.

c. Il riscontro di utilizzo indebito dei Dispositivi Informatici o della mancata applicazione degli ordini di servizio riportati nella presente Policy di Sicurezza dei dati genera un avviso di ordine generale e non personale. Successivamente, solo al persistere del problema, saranno generati avviso e provvedimenti direttamente alle persone afferenti.

## 14. SANZIONI

Per il mancato rispetto o la violazione delle regole contenute nel presente regolamento saranno applicate le sanzioni previste nel CCNL o nei Contratti stipulati tra le parti. Il mancato rispetto è perseguibile anche ai fini di risarcimento di danni subiti.

**Pompeo Tria – Amministratore Unico Fintria s.r.l.**