Politica del Sistema di Gestione Integrato (Qualità, Sicurezza delle Informazioni, Servizi in Cloud e Continuità Operativa)

Controllo delle revisioni

Versione	Redazione	Data	Motivo
01	RSGI	09/04/2018	Prima emissione – Certificazione ISO 27001 –Sicurezza delle Informazioni
02	RSGI	12/02/2019	Integrazione Politica Qualità, e Gestione dei Servizi IT in aggiunta a quella di Sicurezza delle informazioni e Continuità Operativa
03	RSGI	10/02/2020	Integrazione Politica del Cloud con riferimentialle Estensioni ISO 27017 e ISO 27018
04	RSGI	10/01/2022	Revisione in seguito a Riesame

Lista di distribuzione

Ruolo	Nome e Cognome	Firma	Data
Amministratore Delegato	Michele Provenzale		
Resp. Sistema Integrato - RSI	Nicola Palmieri		
Amministratore di Sistema - AM	Carmine Trivigno		
Security Manager - SM	Maurizio Argoneto		

Publisys SPA si rivolge ad imprese, enti pubblici e privati e aziende di ogni dimensione per governarne processi di implementazione, Tuning, gestione.

I principi fondamentali su cui **Publisys SPA** basa il proprio operato sono:

La **Sicurezza,** il **rispetto delle regole e del cliente**, la **gestione per processi** e per progetti, la **trasparenza** nelle relazioni e il **miglioramento continuo**.

Publisys SPA intende offrire ai propri Clienti un "**Servizio a Valore Aggiunto**" ingrado di soddisfare ognuno di loro proponendo le migliori soluzioni globali ICT a specifici problemi, proponendo soluzioni complete che si estendono dallo studio di fattibilità fino alla realizzazione finale e gestione operativa, e impegnandosi per il conseguimento dei requisiti e quindi per la massima soddisfazionedei Clienti stessi.

Per garantire una continua rispondenza ai bisogni espressi dai propri Clienti in fatto di Qualità, Servizi, Sicurezza delle Informazioni, Tutela dell'Ambiente e Continuità Operativa, **Publisys SPA** ha attuato un Sistema di Gestione integrato conforme alle norme **ISO 9001:2015**, **ISO 27001:2013 (**più estensioni **ISO 27017:2015** - **27018:2019), e ISO 22301:2019** garantendo la revisione periodica e il miglioramento continuo di tutti i processi aziendali e servizi erogati tenendo in considerazione, nella definizione delle proprie attività, le necessità e le aspettative dei propri Stakeholder. Relativamente ai Clienti, **Publisys SPA** si impegna a rispettare i vincoli ed i requisiti contrattuali concordati ed esplicitati nella **Business Impact Analysis** condotta sui servizi in perimetro.

L'efficacia, la tempestività e la qualità del portafoglio dei servizi offerti costituiscono il primo obiettivo di **Publisys SPA** da raggiungere attraverso l'attenzione a questi aspetti da parte di ogni singolo collaboratore.

Di conseguenza **Publisys SPA** riconosce nella qualità delle competenze dei propri collaboratori il valore principale su cui fondare la società e s'impegna a realizzare piani di formazione per il personale.

Publisys SPA. ha quindi individuato le seguenti linee guida strategiche:

- stabilire rapporti di partnership con i propri clienti supportandoli nei servizi scelti con le più avanzate soluzioni ICT;
- costruire partnership strategiche con i vendor leader del mercato ICT per essere sempre all'avanguardia nelle soluzioni tecnologiche;
- individuare, reclutare, sviluppare e mantenere i collaboratori attraverso formazione, percorsi di carriera personalizzati e meccanismi innovativi di incentivazione, in modo da accrescere costantemente la qualità delle competenze.

In qualità di erogatore di **Servizi Cloud**, al fine di proteggere le informazioni proprie e dei Clienti archiviate e gestite in Cloud, ha definito una Politica del Cloud specifica per indirizzare al meglio gli obiettivi di Sicurezza delle Informazioni compreso il conseguimento della Certificazione del Sistema di Gestione della Sicurezza delle Informazioni ISO 27001:2013 con estensione ai controlli **ISO 27017:2015** e **ISO 27018:0219.**

Al fine di perseguire gli obiettivi prefissati dalla Direzione di **Publisys SPA**, saranno messe in atto iniziative finalizzate a:

- **Definire**, implementare e mantenere aggiornato ed operativo il **Sistema di Gestione Integrato**, conforme agli standard internazionali **sopra citati**, alla legislazione vigente e alla tutela dei copyright;
- **Sensibilizzare** e formare lo staff su detto Sistema di Gestione Integrato, sui relativi sistemi di riferimento e sulle sanzioni previste in caso di violazione dei contratti di Servizio;
- **Migliorare** continuamente il livello di Servizio, Qualità, Sicurezza delle Informazioni, Tutela Ambientale e Continuità Operativa;
- **Attuare**, ove necessario, idonee azioni correttive per ridurre a livelli ritenuti accettabili l'incidenzadi condizioni anomale sul funzionamento complessivo del sistema;

- **Definire** reazioni idonee al manifestarsi di incidenti di sicurezza per garantire la continuità dell'operatività in sicurezza (**Business Continuity**);
- **le vulnerabilità** dei propri Asset aziendali da minacce quali virus, software nocivo, ecc. tramite interventi di monitoraggio e protezione ad ampio spettro che interessano:
  - sistemi hardware e software (personal computer, workstation, server, supporti di memorizzazione, apparecchiature di rete, sistemi di comunicazione elettronica);
  - informazioni (banche dati, documenti digitali e dati in transito su sistemi di comunicazione);
  - servizi (posta elettronica e accessi al portale).
- **Caratterizzare la propria offerta di servizi** ai Clienti con la garanzia della salvaguardia delle informazioni condivise mediante il monitoraggio sistematico del rispetto delle regole di protezione delle informazioni vigenti in Publisys SPA o definite in sede contrattuale.

- Nell'ambito della **Continuità Operativa**, l'organizzazione mira a realizzare i seguenti obiettivi strategici:
  a) **Garantire la salvaguardia** e la tutela delle vite umane a fronte di un evento di crisi;
  b) **Garantire la continuità operativa** e minimizzare gli impatti sul business in caso di crisi, assicurando un rapido ripristino del normale stato di svolgimento delle attività di business;
  c) **Garantire la resilienza delle architetture** di Publisys SPA;
  d) **Tutelare gli interessi** dell'Organizzazione e aumentare la fiducia dei propri clienti e partner, ponendo particolare attenzione agli aspetti di:
     - ***Disponibilità***: attraverso lo sviluppo e l'implementazione di meccanismi che consentono l'accessibilità e l'usabilità dei servizi quando richiesti da un'entità autorizzata anche a seguito di disastro;
     - ***Livello di Servizio***: attraverso lo sviluppo e l'implementazione di meccanismi che garantiscano la continuità del servizio erogato nel rispetto degli SLA definiti;
     - ***Compliance***: conformità alle prescrizioni di legge e di regolamentazione e ai vincoli di natura contrattuale.
  e) **definire dei piani di continuità operativa**, che include anche quello di Disaster Recovery, che prevedono test ripetuti per garantire l'adeguatezza e l'aggiornamento continuo delle strategie e delle soluzioni tecniche ed organizzative adottate;
  f) **definire e formalizzare una struttura organizzativa**, con ruoli e responsabilità precise in ambito di gestione della continuità Operativa, promuovendo il coinvolgimento di tutte le funzioni aziendali;
  g) **pianificare e assicurare la disponibilità delle risorse** (materiali, umane e in termini di quantità e competenza);
  h) **assicurare** innanzitutto, **la salvaguardia** e **la sicurezza fisica delle persone**, in caso di disastro o di grave incidente;
  i) **prepararsi ad offrire una risposta adeguata** per gestire un'interruzione dei servizi, anche a seguito di disastro;
  j) **migliorare la capacità di resistere** ad incidenti (resilienza) che possono determinare interruzioni di attività critiche;
  k) **effettuare tutte le azioni adeguate** per proteggere il valore aziendale, adempiere ad obblighi di carattere normativo, soddisfare esigenze dei clienti.
- **Migliorare continuamente** il livello di Sicurezza, sia "logica", "Organizzativa" e "Fisica", rispettando le strategie di business, in conformità ai requisiti legali, normativi e contrattuali, tenendo presente i requisiti delle terze parti interessate.
- **Assegnare** e **monitorare** opportuni ruoli e responsabilità per la gestione della sicurezza delle informazioni, della Qualità, del Servizio, dell'Ambiente e Continuità Operativa;
- **Valutare periodicamente i Rischi** di Sicurezza delle Informazioni, Qualità, ambiente, del Servizio ed di Business Continuity e di tutte le parti interessate, al fine di ridurli a livelli accettabili;
- **Aumentare il livello di competenza** e **consapevolezza** della popolazione aziendale sugli aspetti relativi alla sicurezza delle informazioni;
- **Proteggere il proprio patrimonio informativo** e quello delle parti interessate in termini di

Riservatezza, Integrità e Disponibilità;

- **Ottimizzare** l'utilizzo di **Risorse Energetiche**, evitando gli sprechi, e utilizzando le migliori tecnologie disponibili**;**
- **Verificare periodicamente** l'efficacia e l'efficienza del sistema di Gestione Integrato, attraverso **Audit Interni**, garantendo l'adeguato supporto per l'adozione delle necessarie migliorie in base agli obiettivi di business aziendali al fine di garantirne il suo corretto adeguamento;
- **Preservare** al meglio l'immagine aziendale;
- **Assicurare e monitorare i requisiti** di sicurezza all'interno degli accordi con le parti interessate;
- **Ridurre il numero di incidenti** di sicurezza delle informazioni e gli eventi che impattano la Continuità Operativa;
- **Tutelare la salvaguardia dei Dati Personali** trattati in tutte le fasi dei processi aziendali considerando l'Information Security uno strumento che permette la condivisione sicura delle informazioni, il miglioramento delle prestazioni rese ai Clienti e della propria immagine, in linea con le disposizioni del Nuovo Regolamento Europeo 679/2016 in materia di Dati Personali.

In considerazione dell'importanza degli obiettivi da raggiungere e dell'impegno necessario per il loro ottenimento, s'invita tutto lo Staff a prestare la propria collaborazione alla attuazione delle procedure ed alle altre disposizioni in merito eventualmente fornite dalla Direzione.

Tito, 10/01/2022

Nicola Palmieri	**Michele Provenzale**
Predisposizione	**Verifica e Approvazione**
Responsabile Sistema Integrato	**Amministratore Delegato**