ITALPOL VIGILANZA S.R.L.

SEDE GENERALE – ROMA

Via Monte Carmelo, 3

00166 Roma

Tel. +39 06 321 08 41

Fax. +39 06 322 39 29

DOCUMENTO	**POLITICA E OBIETTIVI PER LA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI**
RIFERIMENTI	SGSI ISO 27001; Regolamento Europeo 679/2016;
REVISIONE	Rev. 1 del 30 Gennaio 2020

CONTROLLO DEL DOCUMENTO

TABELLA DI CONTROLLO DELLE REVISIONI		
REV.	DATA	CAUSALE
00	07.01.2019	Prima emissione
01	30.01.2020	Adeguamento rispetto a ultimo Riesame della Direzione

TABELLA DI CONTROLLO DELL'EMISSIONE	
REDAZIONE	Responsabile Sistema di Gestione per la Sicurezza delle Informazioni
VERIFICA	RIT
VERIFICA - APPROVAZIONE	Direttore Generale - RTD

TABELLA DI CONTROLLO DELLA DISTRIBUZIONE DELLE COPIE CONTROLLATE	
NR	SOGGETTI DESTINATARI
1	Direttore Generale - RTD
2	Responsabile Sistema di Gestione Sistema Integrato
3	Responsabile Sistema di Gestione per la Sicurezza delle Informazioni - RIT
4	Responsabili trattamento delle informazioni ai sensi del Regolamento Europeo 679/2016
5	Ente di Certificazione

TABELLA DI CONTROLLO DELL'AGGIORNAMENTO
L'ultima versione di questo documento può essere scaricato dai destinatari autorizzati dalla intranet aziendale o può essere ottenuto mediante richiesta indirizzata tramite email al Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni. L'aggiornamento della copia cartacea è a cura del destinatario, essendo la versione elettronica il documento oggetto di controllo della revisione.

SOMMARIO

0.INTRODUZIONE

ITALPOL VIGILANZA S.R.L. (di seguito: "Azienda") ha come missione strategica l'erogazione di servizi di servizi di vigilanza e servizi di reception e portierato così come descritto dal catalogo dei servizi http://www.italpolvigilanza.it/

In funzione della propria missione strategica, l'Azienda ha pianificato il proprio assetto organizzando una struttura che include l'adozione di specifici sistemi di gestione. In considerazione della missione strategica sopra delineata, assume particolare rilevanza l'adozione di un sistema di gestione per la sicurezza delle informazioni in conformità allo standard ISO 27001 per perseguire i seguenti obiettivi:

- assicurare, anche con riferimento al sistema di gestione per la qualità adottato, la conformità ai requisiti di business dei servizi erogati ai propri clienti;
- assicurare, anche con riferimento ai requisiti in materia di protezione dei dati personali, la conformità alle disposizioni del Regolamento Europeo 679/2016 "privacy".

Nell'ambito del sistema di gestione per la sicurezza delle informazioni adottato dall'Azienda assume particolare rilevanza la definizione, la formalizzazione e l'approvazione da parte della Direzione della politica e degli obiettivi per la sicurezza delle informazioni.

1.SCOPO E CAMPO DI APPLICAZIONE

1.1 SCOPO

Il presente piano descrive la politica per la gestione della sicurezza delle informazioni adottata dall'Azienda ed i relativi obiettivi. In particolare che gli obiettivi siano:

a) congruenti con gli indirizzi espressi dalla presente politica e da correlate politiche di taglio maggiormente operativo;
b) misurabili, dove possibile e/o pertinente;
c) allineati i requisiti per la sicurezza delle informazioni e i risultati della valutazione e del trattamento dei rischi;
d) comunicati;
e) aggiornati in modo appropriato.

1.2 CAMPO DI APPLICAZIONE

Il presente piano si applica ed è quindi richiamato dai seguenti sistemi di gestione adottati dall'Azienda:

- Sistema di Gestione per la Sicurezza delle Informazioni ISO 27001 e del Regolamento Europeo 679/2016 "privacy;

2.NORMATIVA DI RIFERIMENTO

Il presente documento fa riferimento alle seguenti norme:

- standard UNI EN ISO IEC 27001:2013 "Tecnologia per l'Informazione – Tecniche per la Sicurezza – Sistemi di Gestione per la Sicurezza delle Informazioni – Requisiti";
- Regolamento Europeo 679/2016 "privacy

3.TERMINI E DEFINIZIONI

Si riporta la definizione degli acronimi utilizzati nel presente documento:

- SGSI: Sistema di Gestione per la Sicurezza delle Informazioni (secondo lo standard ISO 27001);
- IT: Information Technology.

Si riporta la definizione dei termini utilizzati nel presente documento relativi alla sicurezza delle informazioni:

- **processo**: insieme di attività correlate o interagenti che trasformano elementi in ingresso in elementi in uscita (ISO 9000).
- **informazione**: dati significativi (ISO 9000);

- **sistema di gestione per la sicurezza delle informazioni**: quella parte di sistema di gestione globale, basata su un approccio al rischio aziendale, per istituire, attuare, operare, monitorare, riesaminare, mantenere e migliorare la sicurezza delle informazioni (ISO 27000).
- **sicurezza delle informazioni**: preservazione di riservatezza, integrità e disponibilità delle informazioni. In aggiunta possono essere coinvolte anche altre proprietà quali autenticità, responsabilità, non ripudiabilità e affidabilità (ISO 27000);
- **disponibilità**: la proprietà di essere accessibile e utilizzabile su richiesta di un'entità autorizzata (ISO 27000);
- **riservatezza**: la proprietà per la quale le informazioni non sono rese disponibili o divulgate a individui, entità, o processi non autorizzati (ISO 27000);
- **integrità**: la proprietà di salvaguardare l'accuratezza e la completezza dei beni (ISO 27000);
- **autenticità**: la proprietà che un'entità è ciò che afferma di essere (ISO 27000);
- **responsabilità**: la responsabilità di un'entità per le sue azioni e decisioni (ISO 27000);
- **non ripudiabilità**: capacità di dimostrare il verificarsi di un evento o di una azione e la sua entità originaria, al fine di risolvere le controversie circa il verificarsi o non verificarsi dell'evento o dell'azione e il coinvolgimento delle entità dell'evento (ISO 27000);
- **affidabilità**: proprietà di comportamento previsto coerente ai risultati (ISO 27000).

Si riporta la definizione dei termini utilizzati nel presente documento relativi alla gestione del rischio:

- **bene**: tutto ciò che ha valore per l'organizzazione (ISO 27000).
- **beni sotto forma di informazioni**: conoscenze o dati che hanno valore per l'organizzazione (ISO 27000);
- **gestione del rischio**: attività coordinate per dirigere e controllare un'organizzazione per quanto riguarda il rischio (ISO 27000);
- **rischio**: combinazione della probabilità di un evento e delle sue conseguenze (ISO 27000);
- **rischio sulla sicurezza delle informazioni**: potenzialità che una minaccia possa sfruttare una vulnerabilità di un bene o di un gruppo di beni e quindi possa danneggiare l'organizzazione (ISO 27000);
- **evento**: verificarsi di un particolare insieme di circostanze (ISO 27000);
- **vulnerabilità**: debolezza di un bene o di un controllo che può essere sfruttata da una minaccia (ISO 27000);
- **minaccia**: potenziale causa di un incidente indesiderato, che può provocare danni al sistema o all'organizzazione (ISO 27000);
- **incidente inerente alla sicurezza delle informazioni**: singolo evento inerente alla sicurezza delle informazioni, o una serie di tali eventi, che ha una probabilità significativa di compromettere le operazioni aziendali e di minacciare la sicurezza delle informazioni (ISO 27000);
- **trattamento del rischio**: processo per modificare il rischio (ISO 31000);
- **dichiarazione di applicabilità**: dichiarazione documentata che descrive gli obiettivi del controllo e i controlli che sono pertinenti e applicabili al SGSI dell'organizzazione.
- **obiettivo di controllo**: dichiarazione descrivente ciò che deve essere raggiunto a seguito di controlli da implementare (ISO 27000);
- **controllo**: mezzi di gestione del rischio comprese le politiche, le procedure, le linee guida, le prassi o le strutture organizzative, che possono essere amministrative, tecniche, di gestione o di natura legale (ISO 27000).

Si riporta la definizione dei termini utilizzati nel presente documento relativi alla documentazione:

- **documento**: informazioni con il loro mezzo di supporto (ISO 9000);
- **politica**: indirizzi gestionali formalmente espressi dalla Direzione (ISO 27000);
- **procedura**: modo specificato per svolgere un processo o un'attività (ISO 27000);

4 Politica e Obiettivi

4.1 Obiettivi

L'obiettivo del Sistema di Gestione per la Sicurezza delle Informazioni di Italpol Vigilanza è di garantire un adeguato livello di sicurezza dei dati e delle informazioni nell'ambito dell'erogazione dei servizi di vigilanza e servizi di reception e portierato, attraverso l'identificazione, la valutazione e il trattamento dei rischi ai quali i servizi stessi sono soggetti.

Infatti l'evoluzione tecnologica e i sempre più frequenti attacchi cibernetici mirati alla violazione dei sistemi informativi pubblici e privati evidenziano la crescente necessità di dotarsi di strumenti di mitigazione del rischio di compromissione dell'integrità, disponibilità e riservatezza dei dati

Per cui il Sistema di Gestione per la Sicurezza per le Informazioni di Italpol Vigilanza definisce un insieme di misure organizzative, tecniche e procedurali a garanzia del soddisfacimento dei sotto elencati requisiti di sicurezza di base:

- **RISERVATEZZA**
- **INTEGRITÀ**
- **DISPONIBILITÀ**

In particolare gli obiettivi nell'ambito della sicurezza delle informazioni da perseguire sono quelli che permettono di:

- Rispondere pienamente alle indicazioni della normativa vigente e cogente;
- Ottimizzare i processi di erogazione dei servizi;
- Preservare al meglio l'immagine dell'azienda quale fornitore affidabile e competente;
- Proteggere al meglio il patrimonio informativo proprio e dei propri clienti;
- Adottare le misure atte a garantire la fidelizzazione del personale e la sua professionalità;
- Aumentare, nel proprio personale, il livello di sensibilità e la competenza su temi di sicurezza.
- Fare in modo che tutti i fornitori esterni abbiano consapevolezza dei problemi di sicurezza delle informazioni di Italpol Vigilanza e rispettino la politica di sicurezza adottata;
- Stabilire delle linee guida per l'applicazione di standard, di procedure e di sistemi per realizzare il Sistema di Gestione della Sicurezza delle Informazioni (SGSI);
- Utilizzare gli standard ISO 27001:2013 "Information Security Management Systems — Requirements" e ISO 27002:2013 "Code of practice for information security management" come linee guida della propria sicurezza delle informazioni e perseguirne la conformità;
- Garantire che tutti i collaboratori siano a conoscenza del "Regolamento generale sulla protezione dei dati" e delle relative implicazioni, nonché delle modalità di applicazione delle misure previste, come richiamato nelle procedure operative di sicurezza.
- Garantire che il processo di gestione del rischio informatico adottato da Italpol Vigilanza sia adeguatamente presidiato e periodicamente aggiornato alla luce dei parametri contemplati all'interno della normativa costituente il SGSI.

4.2 Politica

I principi generali cui Italpol Vigilanza si ispira nella gestione della sicurezza si basa sul fatto che ognuno che è coinvolto direttamente o indirettamente nell'erogazione dei servizi di Italpol Vigilanza deve comprendere ed essere consapevole dell'importanza della sicurezza. Quindi:

1. Deve essere creata la massima consapevolezza possibile sui concetti di informazione fisica e digitale e di come queste informazioni debbano essere trattate;
2. Deve essere compreso che le password, e in generale gli account, per l'accesso al sistema informativo aziendale è un segreto che se svelato può mettere in pericolo l'azienda e le persone che ci lavorano
3. Deve essere compreso che la maggior parte delle informazioni sono gestite attraverso varie tecnologie informatiche in grado di dialogare fra loro grazie alle reti di telecomunicazione e quindi potenzialmente un malintenzionato può intercettare queste informazioni se non si presta particolare attenzione;
4. Deve essere compreso che tutti i dispositivi mobili, in particolare smartphone e computer portatili ci permettono di trattare informazioni, anche sensibili, in mobilità e che proprio per questo motivo si è esposti ad altre minacce come ad esempio il furto e per cui è necessario prendere ulteriori precauzioni;

5. Deve essere compreso che i Malware (i software malevoli) possono diffondersi molto facilmente attraverso una moltitudine di mezzi e che quindi bisogna prestare molta attenzione a utilizzare software non previsti dall'azienda, a scaricare file la cui provenienza è incerta
6. Deve essere compreso che i Social Network sono luoghi in cui è molto semplice divulgare informazioni personali e aziendali e arrecare grave danni di reputazione ed esporre noi e la nostra azienda a nuove forme di minacce note come "Social Engineering"
7. Deve essere compreso che una delle principali minacce (il phishing) a sui siamo sottoposti è quella di fornire inconsapevolmente informazioni riservate a malintenzionati semplicemente cliccando su un link da email, sms, tweet ecc.
8. Deve essere compreso che in generale cliccare su un link da email, pagine web, post facebook, ecc, la cui sorgente non è nota può esporci alla minaccia nota come "ransomware" che non ci permette più di accedere ai nostri dati e che questo può portare al fallimento di un'azienda oltre che a recare grave pericolo per la persona
9. Deve essere compreso che ognuno, all'interno di Italpol Vigilanza, deve notificare qualsiasi comportamento anomalo osservato sul proprio PC perché potrebbe essere indice di un sistema compromesso che se non gestito rapidamente potrebbe arrecare grave danno all'azienda;
10. Deve essere compreso che il rischio è parte del business e che cambia con l'evoluzione degli scenari di business, della tecnologia, dei cambi organizzativi. Per questo è necessario attuare un ciclo di miglioramento continuo orientato a verificare che le misure intraprese siano sempre attuali ed adeguate.

9.POLITICA DI CONTROLLO OPERATIVO PER LA SICUREZZA DELLE INFORMAZIONI

Il presente documento definisce la politica per la gestione della sicurezza delle informazioni. In tale ottica, il presente documento può richiamare uno o più documenti di politica di controllo operativo che riportano gli indirizzi definiti dalla Direzione, relativamente a specifiche tematiche per la sicurezza delle informazioni. Tali politiche di controllo operativo sono in genere associate all'implementazione dei controlli previsti dall'Appendice A dello standard ISO 27001 e richiamate dal Piano di Trattamento dei Rischi, documento a cui si rimanda.

- *fine del documento* *-*