AliasLab S.p.A.
Registered office Milano
Via Emilio Cornalia, 11
20124 Milano - Italy

Head Office Mantova
Via Cremona, 27/6
46100 Mantova - Italy
P +39 0376 285101

Branch Office Padova
Galleria Spagna, 19
35127 Padova - Italy
P+39 049 2108800

Sedi certificate
Mantova e Padova

ISO 9001 - ISO 14001
ISO 27001 - ISO 20000
BUREAU VERITAS
Certification

N° IT243263 / N° IT262028/UK
N° IT287326 / N° IND18.0561

Politica

per la qualità, la qualità dei servizi IT e la sicurezza delle informazioni

Informazioni sul documento

REVISIONI			
Rev	**Data**	**Descrizione delle Modifiche**	**Referente**
00	01/06/2015	Prima stesura	Gianluca Buelloni
01	08/09/2016	update	Laura Turetta
02	16/03/2017	Revisione, Integrazione con riferimento alla politica "PO_PPP_01 Politica per la protezione dei dati personali"	Laura Turetta
03	18/10/2018	revisione	Laura Turetta
04	14/03/2019	Aggiornamento template informazioni sul documento	Ilaria Guido

CLASSIFICAZIONE DEL DOCUMENTO					
	UE – Uso esterno/ External use	x	**UI** – Uso interno/ Internal use		**CL** – Circolazione limitata/ Limited circulation

CLASSIFICAZIONE DELLE INFORMAZIONI					
x	**P** – Pubblico		**R** – Riservato/ Confidential		**S** – Segreto/Secret

ACRONIMI E DEFINIZIONI	
SGI	Sistema di Gestione Integrato

REFERENZE E RIFERIMENTI AD ALTRI DOCUMENTI			
Ref.	**Titolo**	**Autore**	**Rev.**

Sommario

Informazioni sul documento 2

1 Riferimenti 4

2 Politica della direzione 4

3 Impegno e obiettivi della direzione 4

4 Campo di applicazione 5

1 Riferimenti

UNI EN ISO 9001:2015 Sistema di gestione per la qualità
ISO/IEC 20000-1:2011 Information Technology – Service management – Service management system requirements
ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements

2 Politica della direzione

La direzione di AliasLab S.p.A. ha definito, ha divulgato e si impegna a mantenere attiva a tutti i livelli della propria organizzazione la presente politica per la Gestione della qualità, della qualità sei servizi IT e della Sicurezza delle Informazioni (di seguito PQSS).
Lo scopo della presente policy è quello di:

- Avere un quadro strutturale di riferimento per definire e riesaminare periodicamente gli obiettivi e per perseguire il miglioramento continuo dell'efficacia del sistema.
- mantenere sotto controllo i processi interni, operare affinché questi risultino efficaci e idonei a realizzare prodotti conformi ai requisiti del cliente ed alle normative cogenti ed a soddisfare le aspettative ed esigenze dei clienti, considerati la prima risorsa dell'azienda stessa
- garantire la tutela e la protezione da tutte le minacce, interne o esterne, intenzionali o accidentali, delle informazioni nell'ambito delle proprie attività in accordo con le indicazioni fornite dallo standard ISO/IEC 27001, nonché dal regolamento europeo GDPR in materia di trattamento dei dati personali per il quale è definita apposita politica "PO_PPP_01 Politica per la protezione dei dati personali"

3 Impegno e obiettivi della direzione

La direzione sostiene attivamente la politica dell'azienda tramite un chiaro indirizzo, un impegno evidente, degli incarichi espliciti e il riconoscimento delle responsabilità relative alla sicurezza delle informazioni.
L'impegno della direzione si attua tramite una struttura i cui compiti sono:

- garantire che siano identificati tutti gli obiettivi relativi al sistema di gestione integrato e che questi incontrino i requisiti aziendali;
- stabilire i ruoli aziendali e le responsabilità per lo sviluppo e il mantenimento del SGI;
- fornire risorse sufficienti alla pianificazione, implementazione, organizzazione, controllo, revisione, gestione e miglioramento continuo del SGI;
- controllare che il SGI sia integrato in tutti i processi aziendali e che procedure e controlli siano sviluppati efficacemente;
- monitorare i cambiamenti dell'esposizione alle minacce delle informazioni chiave dell'azienda e analizzare gli incidenti alla sicurezza, alla qualità e ai servizi IT, rivedendo i criteri per l'accettazione del rischio e i livelli di rischio accettabili; così come gli altri indicatori previsti dal sistema;
- approvare e sostenere tutte le iniziative volte al miglioramento del sistema;
- attivare programmi per la diffusione della consapevolezza e della cultura della sicurezza delle informazioni, della qualità dei servizi IT e della qualità in generale.

4 Campo di applicazione

La presente politica si applica indistintamente a tutti gli organi e i livelli di AliasLab S.p.A.
L'attuazione della presente politica è obbligatoria per tutto il personale e deve essere inserita negli accordi presi con qualsiasi soggetto esterno che, a qualsiasi titolo, possa essere coinvolto.

Per quanto riguarda la sicurezza delle informazioni, il patrimonio informativo da tutelare è costituito dall'insieme delle informazioni gestite attraverso i servizi forniti.
È necessario assicurare:

- la confidenzialità delle informazioni, ovvero le informazioni devono essere accessibili solo da chi è autorizzato.
- l'integrità delle informazioni, ovvero proteggere la precisione e la completezza delle informazioni e dei metodi per la loro elaborazione.
- la disponibilità delle informazioni, ovvero che gli utenti autorizzati possano effettivamente accedere alle informazioni e ai beni collegati nel momento in cui lo richiedono.

La mancanza di adeguati livelli di sicurezza può comportare il danneggiamento dell'immagine aziendale, la mancata soddisfazione del cliente, il rischio di incorrere in sanzioni legate alla violazione delle normative vigenti nonché danni di natura economica e finanziaria.
Un adeguato livello di sicurezza è altresì basilare per la condivisione delle informazioni.
L'azienda identifica tutte le esigenze di sicurezza tramite l'analisi dei rischi che consente di acquisire consapevolezza sul livello di esposizione a minacce del proprio sistema informativo.
La valutazione del rischio permette di valutare le potenziali conseguenze e i danni che possono derivare dalla mancata applicazione di misure di sicurezza al sistema informativo e quale sia la realistica probabilità di attuazione delle minacce identificate.
I risultati di questa valutazione determinano le azioni necessarie per gestire i rischi individuati e le misure di sicurezza più idonee.
I principi generali della gestione della sicurezza delle informazioni abbracciano vari aspetti:

- Deve esistere un catalogo costantemente aggiornato degli asset aziendali rilevanti ai fini della gestione delle informazioni e per ciascuno deve essere individuato un responsabile.
- Le informazioni devono essere classificate in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza ed integrità coerenti ed appropriati.
- Per garantire la sicurezza delle informazioni, ogni accesso ai sistemi deve essere sottoposto a una procedura d'identificazione e autenticazione.
- Le autorizzazioni di accesso alle informazioni devono essere differenziate in base al ruolo ed agli incarichi ricoperti dai singoli individui, in modo che ogni utente possa accedere alle sole informazioni di cui necessita, e devono essere periodicamente sottoposte a revisione.
- Devono essere definite delle procedure per l'utilizzo sicuro dei beni aziendali e delle informazioni e dei loro sistemi di gestione.
- Deve essere incoraggiata la piena consapevolezza delle problematiche relative alla sicurezza delle informazioni in tutto il personale (dipendenti e collaboratori) a partire dal momento della selezione e per tutta la durata del rapporto di lavoro.

- Per poter gestire in modo tempestivo gli incidenti, tutti devono notificare qualsiasi problema relativo alla sicurezza. Ogni incidente deve essere gestito come indicato nelle procedure.
- È necessario prevenire l'accesso non autorizzato alle sedi e ai singoli locali aziendali dove sono gestite le informazioni e deve essere garantita la sicurezza delle apparecchiature.
- Deve essere assicurata la conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni nei contratti con le terze parti.
- Deve essere predisposto un piano di continuità che permetta all'azienda di affrontare efficacemente un evento imprevisto, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino le conseguenze negative sulla missione aziendale.
- Gli aspetti di sicurezza devono essere inclusi in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici.
- Devono essere garantiti il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente la sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni alla reputazione.

L'osservanza e l'attuazione di questa policy sono responsabilità di tutto il personale che, a qualsiasi titolo, collabora con l'azienda ed è in qualche modo coinvolto con il trattamento di informazioni che rientrano nel campo di applicazione del Sistema di Gestione della Sicurezza delle Informazioni.
Tutto il personale è altresì responsabile della segnalazione di tutte le anomalie e violazioni di cui dovesse venire a conoscenza.

Tutti i soggetti esterni che intrattengono rapporti e collaborano con l'azienda devono garantire il rispetto dei requisiti di sicurezza contenuti nella presente policy.
Il Responsabile del sistema deve:

- condurre l'analisi dei rischi con le opportune metodologie e adottare tutte le misure per la gestione del rischio
- stabilire tutte le norme necessarie alla conduzione sicura di tutte le attività aziendali
- verificare le violazioni alla sicurezza e adottare le contromisure necessarie e controllare l'esposizione dell'azienda alle principali minacce
- organizzare la formazione e promuovere la consapevolezza del personale per tutto ciò che concerne la sicurezza delle informazioni
- verificare periodicamente l'efficacia e l'efficienza del Sistema di Gestione della Sicurezza delle Informazioni.

Chiunque, dipendenti, consulenti e/o collaboratori esterni dell'Azienda, in modo intenzionale o riconducibile a negligenza, disattenda le regole di sicurezza stabilite e in tal modo provochi un danno all'azienda, potrà essere perseguito nelle opportune sedi e nel pieno rispetto dei vincoli di legge e contrattuali.
La Direzione verificherà periodicamente e regolarmente o in concomitanza di cambiamenti significativi l'efficacia e l'efficienza del Sistema di Gestione Integrato, in modo da assicurare un supporto adeguato all'introduzione di tutte le migliorie necessarie e in modo da favorire l'attivazione di un processo continuo, con cui viene mantenuto il controllo e l'adeguamento della policy in risposta ai cambiamenti dell'ambiente aziendale, del business, delle condizioni legali.
Il Responsabile del SGI ha la responsabilità del riesame della presente politica. Il riesame dovrà verificare lo stato delle azioni intraprese, le azioni correttive, l'aderenza alla politica e analizzare l'andamento dei piani di miglioramento. Dovrà inoltre tenere conto di tutti i cambiamenti che possono influenzare l'approccio della azienda alla gestione del SGI, includendo i cambiamenti organizzativi, l'ambiente tecnico, la disponibilità di risorse, le condizioni legali, regolamentari o contrattuali e dei risultati dei precedenti riesami. Particolare attenzione sarà prestata agli incidenti segnalati relativi alla sicurezza delle informazioni e alle tendenze relative alle minacce e vulnerabilità.
Il risultato del riesame dovrà includere tutte le decisioni e le azioni relative al miglioramento dell'approccio aziendale alla gestione del SGI, dei controlli e nell'allocazione delle risorse e delle responsabilità.